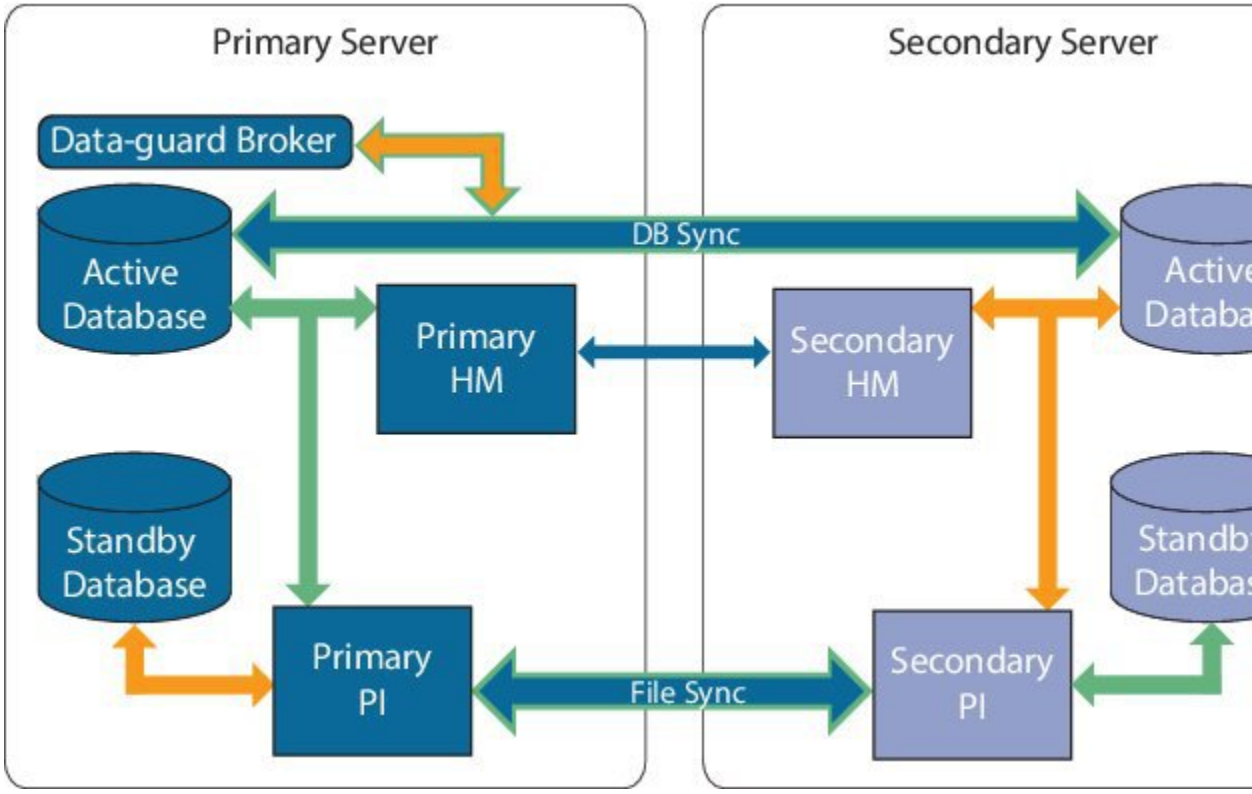
ハイ アベイラビリティの設定

ハイ アベイラビリティの仕組み

以下の図に、Prime Infrastructure ハイ アベイラビリティ（HA）をセットアップしてプライマリ サーバーをアクティブにするための主要コンポーネントとプロセス フローを示します。

図 *1 : HA* の導入



HA の導入には、2 台の Prime Infrastructure サーバー（プライマリとセカンダリ）が必要です。これらのサーバーのそれぞれに、アクティブ データベースとアクティブ データベースのスタンバイ バックアップ コピーがあります。通常状態では、プライマリ サーバーがアクティブです。つまり、プライマリ サーバーが自身のアクティブ データベースに接続されており、ネットワークを管理します。セカンダリ サーバーはパッシブ状態で、自身のスタンバイ データベースのみに接続されていますが、プライマリ サーバーとは継続的な通信状態にあります。

両方のサーバーで実行されているヘルス モニター プロセスにより、お互いのサーバーのステータスがモニターされています。両方のサーバー上で実行されている Oracle Recovery Manager（RMAN）は、アクティブ データベースおよびスタンバイ データベースを作成し、変更の発生時には、プライマリ サーバーで実行される Oracle Data Guard Broker の効果によりデータベースを同期します。

プライマリ サーバーに障害が発生すると、セカンダリが引き継ぎ、自身のアクティブ データベースに接続します。このデータベースは、アクティブ プライマリ データベースと同期されています。この切り替えは「フェールオーバー」と呼ばれ、手動（推奨）または自動でトリガーできます。その後は、プライマリ サーバーへのアクセスの復元作業をしながら、セカンダリ サーバーを使用してネットワークを管理します。プライマリ サーバーが再度使用可能になると、プライマリ サーバーに戻すための切り替え（「フェールバック」）を開始し、プライマリを使用してネットワーク管理を再開できます。

プライマリ サーバーとセカンダリ サーバーを同一 IP サブネットに導入する場合は、1 つの仮想 IP アドレスで Prime Infrastructure に通知を送信するようにデバイスを設定できます。ディザ

スタ リカバリの実施などの目的で、2 台のサーバーを地理的に離れた位置に分散する場合は、両方のサーバーに通知を送信するようにデバイスを設定する必要があります。

関連トピック

プライマリ サーバーとセカンダリ サーバーについて （3 ページ）
障害の原因 （3 ページ）
ファイルおよびデータベースの同期 （4 ページ）
HA サーバー通信 （4 ページ）
ヘルス モニター プロセス （5 ページ）
ヘルス モニター Web ページ （5 ページ）
HA での仮想 IP アドレッシングの使用 （8 ページ）
HA 環境で SSL 証明書を使用する方法 （9 ページ）
Web ブラウザへのクライアント証明書のインポート （9 ページ）

プライマリ サーバーとセカンダリ サーバーについて

すべての Prime Infrastructure HA 実装には、プライマリ サーバーの特定のインスタンスに対して専用のセカンダリ サーバーが 1 台のみ必要です。

通常、HA サーバーごとに独自の IP アドレスまたはホスト名が設定されています。同一サブネット上に配置されているサーバーは、仮想 IP を使用して同じ IP を共有できます。これにより、デバイスの設定が容易になります。Prime Infrastructure のプライマリおよびセカンダリ サーバーは、HA 実装時にネットワーク インターフェイス ethernet0（eth0）で有効にする必要があります。

HA をセットアップした後は、HA サーバーの IP アドレスやホスト名を変更しないください。変更すると、HA 設定が失われます（「関連項目」の「サーバーの IP アドレスまたはホスト名のリセット」を参照）。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
HA での仮想 IP アドレッシングの使用 （8 ページ）
HA サーバーの IP アドレスまたはホスト名のリセット （59 ページ）

障害の原因

Prime Infrastructure サーバーの障害は、以下の 1 つ以上の分野での問題が原因で発生する可能性があります。

- **アプリケーション プロセス**：NMS サーバー、MATLAB、TFTP、FTP を含め、1 つ以上の Prime Infrastructure サーバー プロセスが失敗した場合。各アプリケーション プロセスの動作ステータスを確認するには、管理コンソールから ncs status コマンドを実行します。
- **データベース サーバー**：1 つ以上のデータベース関連のプロセスがダウンした場合。データベース サーバーは、Prime Infrastructure 内のサービスとして実行されます。
- **ネットワーク**：ネットワーク アクセスの問題や、到達可能性の問題が発生した場合。

- **システム**：サーバーの物理ハードウェアまたはオペレーティング システムに関連する問題が発生した場合。
- **仮想マシン**（VM）：プライマリ サーバーとセカンダリ サーバーがインストールされている VM 環境に問題が発生した場合（HA が VM 環境で稼動している場合）。

詳細については、「ハイ アベイラビリティの仕組み」を参照してください。

ファイルおよびデータベースの同期

HA コンフィギュレーションが、プライマリ サーバーでの変更を判別すると、常にその変更がセカンダリ サーバーに同期されます。これらの変更には、次の 2 種類があります。

1. **データベース**：コンフィギュレーション、パフォーマンス、およびモニタリング データに関連するデータベースの更新などです。
2. **ファイル**：コンフィギュレーション ファイルに対する変更などです。

両方のサーバー上で実行されている Oracle Recovery Manager（RMAN）は、アクティブ データベースおよびスタンバイ データベースを作成し、変更の発生時には、プライマリ サーバーで実行される Oracle Data Guard Broker の効果によりデータベースを同期します。

ファイルの変更内容は、HTTPS プロトコルを使用して同期されます。ファイルの同期は、以下のいずれかの方法で行われます。

- **バッチ**：このカテゴリには、頻繁に更新されないファイル（ライセンス ファイルなど）が含まれます。これらのファイルは、500 秒間隔で同期されます。
- **ほぼリアルタイム**：頻繁に更新されるファイルは、このカテゴリに分類されます。これらのファイルは、11 秒間隔で同期されます。

デフォルトでは、HA フレームワークは、必要なすべての構成データをコピーするように設定されます。これらの構成データには、以下が含まれます。

- レポート設定
- コンフィギュレーション テンプレート
- TFTP ルート
- 管理設定
- ライセンス ファイル

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）

HA サーバー通信

プライマリおよびセカンダリ HA サーバーは、HA システムのヘルスを維持するために、次のメッセージを交換します。

- データベース同期：プライマリ サーバーとセカンダリ サーバー上のデータベースが稼働および同期するために必要なすべての情報が含まれます。

- ファイル同期：頻繁に更新されるコンフィギュレーション ファイルが含まれます。これらのファイルは11秒間隔で同期され、他の頻繁に更新されないコンフィギュレーション ファイルは 500 秒間隔で同期されます。
- プロセス同期：アプリケーションおよびデータベースに関連するプロセスの実行が継続されるようにします。これらのメッセージは、ハートビート カテゴリに分類されます。
- Health Monitor 同期：これらのメッセージは、以下の障害状態の有無を確認します。
  - ネットワーク障害
  - システム障害（サーバー ハードウェアとオペレーティング システムでの障害）
  - ヘルス モニター障害

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）

ヘルス モニター プロセス

Health Monitor（HM）とは、HA 操作を管理する主要コンポーネントです。プライマリ サーバーとセカンダリ サーバーでは、それぞれ別個の HM インスタンスがアプリケーション プロセスとして実行されます。HM は、以下の役割を果たします。

- HA に関連するデータベースおよび構成データを同期します（Oracle Data Guard を使用して別途同期されるデータベースは除きます）。
- プライマリ サーバーとセカンダリ サーバーの間で 5 秒間隔でハートビート メッセージを交換し、サーバー間の通信が維持されていることを確認します。
- 両方のサーバー上で使用可能なディスク容量を定期的に確認し、ストレージ容量が不足している場合にはイベントを生成します。
- リンクされた HA サーバー全体のヘルスを管理、制御、モニターします。プライマリ サーバーで障害が発生した場合にセカンダリ サーバーをアクティブ化するのは、Health Monitor の役目です。

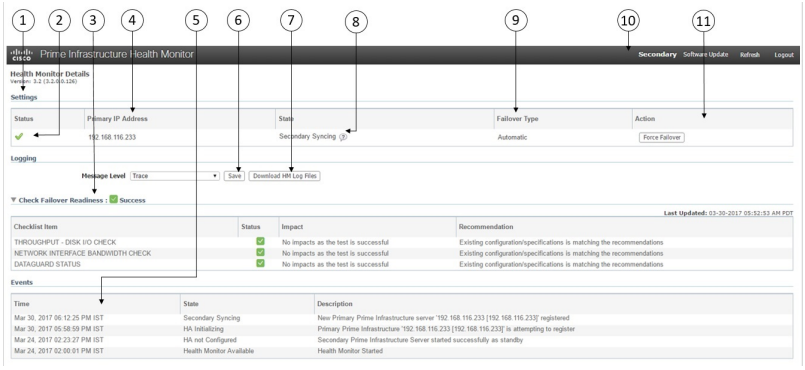
関連トピック

ハイ アベイラビリティの仕組み （1 ページ）

ヘルス モニター Web ページ

Health Monitor Web ページを使用して HA の動作を制御します。プライマリ サーバーまたはセカンダリ サーバーで実行される Health Monitor インスタンスごとに、専用の Web ページがあります。次の図に、「プライマリ アクティブ」状態と「セカンダリ同期中」状態にあるセカンダリ サーバーのヘルス モニター Web ページの例を示します。

図 *2:* ヘルス モニター *Web* ページ（セカンダリ サーバー）



1	[設定（Settings）] 領域に、ヘルス モニターの状態と設定の詳細情報を示す 5 つのセクションが表示されています。
2	[Status] は、HA セットアップの現在の機能ステータスを示します（緑色のチェック マークは、HA がオンであり機能していることを実行します）。
3	[フェールオーバーの準備状況の確認（Check Failover Readiness）] フィールドに、チェックリスト項目のシステム フェールバックの値とシステム フェールオーバーの詳細が表示されます。 詳細については、表の下の「フェールオーバーの準備状況の確認」を参照してください。
4	[プライマリ IP アドレス（Primary IP Address）] は、このセカンダリ サーバーのピア サーバーの IP を示します（プライマリ サーバーの場合、このフィールドには [セカンダリ IP アドレス（Secondary IP Address）] というラベルが付いています）。
5	[イベント（Events）] 表には、現在のすべての HA 関連イベントが最新のイベントを先頭に時系列順に表示されます。
6	[Message Level] フィールドでは、ログ レベル（[Error]、[Informational]、[Trace]）を変更できます。ログ レベルを変更するには、[保存（Save）] をクリックする必要があります。
7	[ロギング ダウンロード（Logging Download）] 領域では、ヘルス モニター ログ ファイルをダウンロードできます。
8	[状態（State）] は、この Health Monitoring インスタンスが実行されているサーバーの現在の HA の状態を示します。
9	[フェールオーバー タイプ（Failover Type）] は、設定されているフェールオーバー タイプ（[手動（Manual）] または [自動（Automatic）]）を示します。
10	表示している Health Monitor Web ページの対象 HA サーバーを示します。

11	[アクション（Actions）]は、実行できるアクション（フェールオーバーまたはフェールバック）を示します。[アクション（Actions）] のボタンは、HA 状態の変更が必要なアクションが Health Monitor により検出された場合にだけ有効になります。

[フェールオーバーの準備状況の確認（Check Failover Readiness）] セクションの説明：

チェックリスト名	説明
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリ サーバーとセカンダリ サーバーの両方でディスク IOPS を検証します。 必要な最小ディスク IOPS は 200 Mbps です。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	プライマリ サーバーとセカンダリ サーバーの両方で eth0 インターフェイス速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - ネットワーク帯域幅速度の確認（NETWORK - CHECK NETWORK BANDWIDTH SPEED）	プライマリ サーバーとセカンダリ サーバーの両方でネットワーク帯域幅速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバーの間でデータを送信することによってネットワーク帯域幅を測定します。 （注） Cisco Prime Infrastructure では、ネットワーク帯域幅の速度テストは Mbps でのみ計算されます。そのため、GBps、MBps、KBps、および Mbps は Mbps に変更され、速度テストへの入力として指定されます。
データベース - 同期ステータス（DATABASE - SYNC STATUS）	プライマリ データベースとセカンダリ データベースを同期する Oracle Data Guard Broker の設定を確認します。

フェールオーバー準備状況の確認に関する傾向グラフ：

- 傾向グラフの [ここをクリック（Click here）] リンクをクリックして、すべてのフェールオーバー準備状況の確認テストに関する傾向グラフを確認します。傾向グラフには、テストの履歴サマリーとシステム/ネットワークの安定性に関するステータスが示されます。
- [日付範囲の選択（Select Date Range）] をクリックして日付と時刻を変更し、[適用（Apply）] をクリックします。デフォルトでは、過去 6 時間の値が傾向グラフに表示されます。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
データベースの同期の問題を解決する方法 （51 ページ）

HA での仮想 IP アドレッシングの使用

通常の状況下では、Prime Infrastructure を使用して、管理対象デバイスがその syslog、SNMP トラップ、およびその他の情報を Prime Infrastructure サーバーの IP アドレスに送信するように設定します。HA を実装する場合、それぞれ異なる IP アドレスを持つ 2 台の Prime Infrastructure サーバーが導入されます。プライマリ サーバーと同様にセカンダリ サーバーにも通知を送信するようにデバイスを再設定しないと、セカンダリ Prime Infrastructure サーバーがアクティブモードになったときに、セカンダリ サーバーではすべての通信が受信されません。

管理対象デバイスすべてで2台の別個のサーバーに通知を送信するよう設定する場合、追加のデバイス設定作業が必要です。この追加のオーバーヘッドを回避するため、HA では両方のサーバーが管理アドレスとして共有できる仮想IPアドレスの使用がサポートされています。フェールオーバー プロセスとフェールバック プロセスの実行中に、この 2 台のサーバーは必要に応じて IP を切り替えます。仮想 IP アドレスは常に、正しい Prime Infrastructure サーバーを指し示します。

両方の HA サーバーのアドレスおよび仮想 IP がすべて同じサブネット上にない場合、仮想 IP アドレッシングを使用できないことに注意してください。これは、HA サーバー導入の選択方法に影響する可能性があります（「関連項目」の「HA の導入計画」および「ローカル モデルの使用」参照）。

また、仮想 IP アドレスを 2 つのサーバー IP アドレスの代わりとして使用することは一切意図されていないことに注意してください。仮想 IP は、syslog やトラップなど Prime Infrastructure サーバーに送信されるデバイス管理メッセージの宛先として使用されます。デバイスのポーリングは、2 つの Prime Infrastructure サーバー IP アドレスのうちの 1 つから常に実施されます。このことを考慮すると、仮想 IP アドレッシングを使用している場合、3 つすべてのアドレス（仮想 IP アドレスおよび 2 つの実際のサーバー IP）における着信および発信 TCP/IP 通信に対してファイアウォールを開く必要があります。

オペレーション センターでの HA の使用を計画している場合、仮想 IP アドレッシングを使用することもできます。オペレーション センターが有効になっている Prime Infrastructure インスタンスに仮想 IP を SSO として割り当てることができます。オペレーション センターを使用して管理されているインスタンスには、仮想 IP は必要ありません（「オペレーション センター用の HA の有効化」を参照）。

プライマリ サーバーでの HA の登録時に仮想 IP アドレッシングを有効にできます。そのためには、この機能を使用する旨を指定し、プライマリ サーバーとセカンダリ サーバーで共有する仮想 IPv4（必要な場合は IPv6）アドレスを入力します（「プライマリ サーバーでの HA の登録方法」を参照）。

仮想 IP アドレッシングを有効化した後に仮想 IP アドレッシングを削除するには、HA を完全に削除する必要があります（「GUI での HA の削除」を参照）。

関連トピック

仮想 IP アドレッシングを使用できない場合の対処 （14 ページ）
HA の導入計画 （10 ページ）
ローカル モデルの使用 （12 ページ）
オペレーション センター用の HA の有効化 （16 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
ハイ アベイラビリティの仕組み （1 ページ）
GUI での HA の削除 （56 ページ）

HA 環境で SSL 証明書を使用する方法

Prime Infrastructure サーバーとユーザー間の通信をセキュアなものにするために SSL 認証を使用することを決め、HA の実装も計画している場合、プライマリ HA サーバーとセカンダリ HA サーバー用に別々の証明書を生成する必要があります。

これらの証明書は、各サーバーの FQDN（完全修飾ドメイン名）を使用して生成する必要があります。つまり、プライマリ サーバーで使用する予定の証明書の生成にはプライマリ サーバーの FQDN を使用し、セカンダリ サーバーで使用する予定の証明書の生成にはセカンダリ サーバーの FQDN を使用する必要があります。

証明書を生成したら、各サーバーに署名付き証明書をインポートします。

仮想 IP アドレスを使用して SSL 証明書を生成しないでください。仮想 IP アドレス機能は、Prime Infrastructure とネットワーク デバイス間の通信を可能にするために使用します。

Cisco Prime Infrastructure の HTTPS アクセスを設定するには、「Prime Infrastructure への HTTPS アクセスをセットアップする」を参照してください。

Web ブラウザへのクライアント証明書のインポート

証明書認証が設定された Prime Infrastructure サーバーにアクセスするユーザーは、認証用にクライアント証明書をブラウザにインポートする必要があります。このプロセスは各種ブラウザで同様ですが、実際の詳細部分についてはブラウザによって異なります。以下の手順では、ユーザーが Prime Infrastructure 互換の Firefox を使用しているものとしています。

クライアント証明書をインポートするユーザーに関して、以下について確認する必要があります。

- クライアント マシンのローカル ストレージ リソースに証明書ファイルのコピーをダウンロード済みであること。
- 証明書ファイルが暗号化されている場合は、証明書ファイルの暗号化に使用されたパスワードを保有していること。

ステップ 1 Firefox を起動し、次の URL をロケーション バーに入力します：**about:preferences#advanced**

Firefox の [オプション（Options）] > [詳細設定（Advanced）] タブが表示されます。

ステップ 2 [証明書（Certificates）] > [証明書の表示（View Certificates）] > 自分の証明書の順に選択して [インポート...（Import...）] をクリックします。.

ステップ 3 ダウンロードした証明書ファイルに移動してそれらを選択し、[OK] または [開く（Open）] をクリックします。

ステップ 4 証明書ファイルが暗号化されている場合、証明書ファイルの暗号化に使用されたパスワードの入力が求められます。該当するパスワードを入力し、[OK] をクリックします。

これで証明書がブラウザにインストールされました。

ステップ 5 Ctrl+Shift+Del を押して、ブラウザのキャッシュをクリアします。

ステップ 6 証明書認証を使用してブラウザで Prime Infrastructure サーバーにアクセスします。

要求されたサーバー認証に応答するための証明書の選択が求められます。適切な証明書を選択し、[OK] をクリックします。

ホット スタンバイ動作

プライマリ サーバがアクティブ状態のとき、セカンダリ サーバは、プライマリ サーバと常時同期状態にあり、高速で切り替えができるように、すべての Prime Infrastructure プロセスを実行しています。プライマリ サーバに障害が発生すると、セカンダリ サーバがフェールオーバー後 2 ～ 3 分以内にアクティブなロールを素早く引き継ぎます。

プライマリ サーバでの問題が解消され、プライマリ サーバが実行状態に戻ると、プライマリ サーバがスタンバイ ロールになります。プライマリ サーバがスタンバイ ロールになると、ヘルス モニタの GUI には「Primary Syncing」状態が表示され、プライマリ サーバ上のデータベースおよびファイルとアクティブなセカンダリ サーバとの同期が開始されます。

プライマリ サーバが再度使用可能になり、フェールバックがトリガーされると、再度プライマリ サーバがアクティブ ロールを引き継ぎます。このようなプライマリ サーバーとセカンダリ サーバー間でのロールの切り替えは、2 ～ 3 分以内に実行されます。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）

HA の導入計画

Prime Infrastructure の HA 機能は、以下の導入モデルをサポートしています。

- **ローカル**：HA サーバーの両方を同じサブネットに配置します（サーバーにレイヤ 2 近接性を与えます）。通常は、両方のサーバーが同じデータ センター内に配置されます。
- **キャンパス**：HA サーバーのそれぞれを、LAN で接続された異なるサブネットに配置します。通常、これらのサーバーは同じ 1 つのキャンパスに導入されますが、キャンパス内で配置される場所は異なります。

- **リモート**：HA サーバーのそれぞれを、WAN で接続された異なるリモート サブネットに配置します。各サーバーが、異なる施設に配置されます。これらの施設は、国や大陸間にまたがり、地理的に分散されています。

以降の項で、各モデルの利点および欠点と、すべての導入モデルに影響する基本的な制約事項について説明します。

HA は、サポートされているいずれの導入モデルでも機能します。主な制約事項は、HA のパフォーマンスと信頼性に関して存在し、これらは帯域幅と遅延の基準によって異なります（「HA のネットワーク スループットに関する制限事項」参照）。これらのパラメータを正常に管理できる限り、使用可能な導入モデルのどれを選んで実装するかは、（コスト、企業の規模、地理、コンプライアンス標準などのビジネスパラメータに基づく）ビジネス上の意思決定です。

関連トピック

HA のネットワーク スループットに関する制限事項 （11 ページ）
ローカル モデルの使用 （12 ページ）
キャンパス モデルの使用 （13 ページ）
リモート モデルの使用 （14 ページ）
仮想 IP アドレッシングを使用できない場合の対処 （14 ページ）
自動フェールオーバーと手動フェールオーバーの違い （15 ページ）
オペレーション センター用の HA の有効化 （16 ページ）

HA のネットワーク スループットに関する制限事項

Prime Infrastructure の HA パフォーマンスは、常に以下の制限要因の影響を受けます。

- すべての操作を処理するために Prime Infrastructure で利用できる正味の帯域幅。これらの操作には、HA 登録、データベース同期、ファイル同期、フェールバックのトリガーが含まれます（ただし、これらに限定されません）。
- プライマリ サーバーとセカンダリ サーバー間のリンク全体における正味のネットワーク遅延。この 2 台のサーバーの物理的な近接性にかかわらず、サーバー間のリンクで発生する遅延が大きい場合、Prime Infrastructure によるプライマリ サーバーとセカンダリ サーバー間のセッション維持状態に影響が及ぶ可能性があります。
- プライマリ サーバーとセカンダリ サーバーを接続するネットワークが提供できる正味のスループット。正味のスループットは正味の帯域幅と遅延によって異なり、これら 2 つの要因の関数と見なすことができます。

モデルによって問題の大きさが異なりますが、これらの制限は、少なくとも何らかのレベルであらゆる導入モデルに当てはまります。例えば、リモート導入モデルは、地理的な分散が大きいため、帯域幅と遅延の両方で問題が発生しがちです。一方、ローカル モデルとキャンパス モデルの場合も、正しく構成されていなければ、帯域幅の問題が発生する可能性が高くなります。これは、低帯域幅、高遅延、高ネットワーク使用率によって制限を受ける可能性があるためです。

スループットの問題がフェールバックやフェールオーバーに影響することはほとんどありません。2 つの HA サーバーがほとんど常に通信して、データベースの変更内容が即座に複製されるためです。ほとんどのフェールオーバーおよびフェールバックは、約 2 ～ 3 分を要します。

この原則の最大の例外は、データベースのフル コピー動作における遅延です。この種類のアクションは、プライマリ サーバーがデータ保持期間を超えてダウンした後、これを再度稼働させる場合にトリガーされます。Express、Express-Plus、Standard の各構成サーバーのデータ保持期間は 6 時間で、Professional および Gen 2 アプライアンス サーバーでは 12 時間です。

Prime Infrastructure はセカンダリ サーバーからプライマリ サーバーへのデータベースのフル コピー動作をトリガーします。この期間中のフェールバックはできませんが、[ヘルス モニター（Health Monitor）] ページには、データベースのコピー進行中に発生したすべてのイベントが表示されます。コピーが完了するとすぐに、プライマリ サーバーは「プライマリ同期中（Primary Synching）」状態に移行し、その後、フェールバックのトリガーが可能になります。データベースのフル コピーが行われている間は、プライマリ サーバーの再起動やネットワーク接続切断を行わないでください。

データベースのフル コピー動作中の正味スループットの変動は、データベースのサイズやその他の要因とは無関係に、データベースのフル コピー動作が 1 時間未満で正常に完了するケースと、まったく完了できないケースという違いを生じるぐらいの意味を持ちます。シスコでは、標準的なデータベース サイズである 105 GB ～ 156 GB の Prime Infrastructure を使用して、以下のリモート モデルの構成での HA 導入における正味スループットの影響をテストしてきました。これらのテストに基づき、シスコでは、125 GB の標準的なデータベース（10 GB のバックアップ ファイルを生成）に対して、以下のように推奨します。

- 最適な結果の場合：サブミリ秒の遅延と 977 Mbps の正味スループットにおいて、データベースのフル コピーの時間を 1 時間未満と想定。
- 良好な結果の場合：70 ミリ秒の遅延と 255 Mbps 以上の正味スループットにおいて、データベースのフル コピーの時間を 2 時間未満と想定。
- 許容可能な結果の場合：220 ミリ秒以下の遅延と 86 Mbps 以上の正味スループットにおいて、データベースのフル コピーの時間を 4.5 時間未満と想定。

遅延が 330ms 以上、スループットが 46Mbps 以下の場合、データベースのコピーが正常に完了しない危険があります。

関連トピック

HA の導入計画 （10 ページ）
リモート モデルの使用 （14 ページ）

ローカル モデルの使用

ローカル導入モデルの主要なメリットは、仮想 IP アドレスをシステムの単一管理ドレスとして使用することが許可される点です。ユーザーはこの仮想 IP アドレスを使用して Prime Infrastructure に接続し、デバイスではこの仮想 IP アドレスを SNMP トラップおよびその他の通知の宛先として使用できます。

仮想 IP アドレスを割り当てる際の唯一の制約は、仮想 IP アドレスが、プライマリ サーバーの IP アドレスおよびセカンダリ サーバーの IP アドレスと同じサブネット上のアドレスでなければならない点です。例：プライマリ サーバーとセカンダリ サーバーに対し、1 つのサブネット内の次の IP アドレスが割り当てられている場合、この両方のサーバーの仮想 IP アドレスは次のように割り当てることができます。

- サブネット マスク：255.255.255.224 (/27)
- プライマリ サーバーの IP アドレス：10.10.101.2
- セカンダリ サーバーの IP アドレス：10.10.101.3
- 仮想 IP アドレス：10.10.101.[4-30]（例：10.10.101.4）仮想 IP アドレスは、特定のサブネットマスクで有効かつ未使用のアドレス範囲内の任意のアドレスになることに注意してください。

この主な利点に加え、ローカル モデルには以下の利点もあります。

- 通常、高帯域幅と低遅延を実現します。
- 管理が簡素化されます。
- syslog および SNMP 通知を転送するようにデバイスを設定するのが、大幅に簡単になります。

ローカル モデルには、以下の欠点があります。

- 同じデータ センター内に配置されることから、停電や自然災害など、サイト全体の障害の危険にさらされます。
- 破壊的なサイト障害の危険が高くなることから、ビジネス継続性の計画が複雑になります。また、損害保険のコストも高くなる可能性があります。

関連トピック

HA の導入計画 （10 ページ）
キャンパス モデルの使用 （13 ページ）
リモート モデルの使用 （14 ページ）

キャンパス モデルの使用

キャンパス モデルでは、HA を導入する組織が、同じ都道府県の同じ市区町村内の 1 つ以上のロケーションを拠点にしていて、これらの複数ロケーションによって「キャンパス」を形成していることが前提となります。このモデルには、以下の利点があります。

- 通常、ローカル モデルに匹敵するか、それ以上の帯域幅と遅延を提供します。
- リモート モデルより簡単に管理できます。

キャンパス モデルには、以下の欠点があります。

- ローカル モデルより、管理が複雑になります。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用することを許可しないでください。その場合は、多くのデバイス設定が必要となります（「関連項目」の「仮想 IP アドレッシングを使用できない場合の対処」参照）。
- ローカルモデルと比べると、帯域幅が小さくなり、遅延が大きくなる可能性があります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「関連項目」の「HA のネットワーク スループットに関する制限事項」参照）。
- 同じサイトに配置されてはいませんが、それでも都道府県全体、または市区町村全体の災害の危険にさらされます。そのため、ビジネス継続性の計画が複雑になり、災害復旧のコストが高くなる可能性があります。

関連トピック

HA の導入計画 （10 ページ）
HA のネットワーク スループットに関する制限事項 （11 ページ）
ローカル モデルの使用 （12 ページ）
リモート モデルの使用 （14 ページ）
仮想 IP アドレッシングを使用できない場合の対処 （14 ページ）

リモート モデルの使用

リモートモデルでは、導入する組織に複数のサイトまたはキャンパスがあること、そしてこれらのロケーション間では、地理的な境界を超えて WAN リンクで通信することが前提となります。このモデルには、以下の利点があります。

- 自然災害による影響を受ける可能性が最小限になります。ビジネス継続性および災害復旧という点では、通常、これが最も複雑でなく、コストのかからないモデルになります。
- 事業保険のコストを節約できる可能性があります。

リモート モデルには、以下の欠点があります。

- ローカルまたはキャンパス モデルより、管理が複雑です。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用することを許可しないでください。その場合は、多くのデバイス設定が必要となります（「関連項目」の「仮想 IP アドレッシングを使用できない場合の対処」参照）。
- 通常、他の2つのモデルよりも提供される帯域幅が低く、遅延が大きくなります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「関連項目」の「HA のネットワーク スループットに関する制限事項」参照）。

関連トピック

HA の導入計画 （10 ページ）
HA のネットワーク スループットに関する制限事項 （11 ページ）
ローカル モデルの使用 （12 ページ）
キャンパス モデルの使用 （13 ページ）
仮想 IP アドレッシングを使用できない場合の対処 （14 ページ）

仮想 IP アドレッシングを使用できない場合の対処

選択する導入モデルによっては、仮想IPアドレスを設定しないでおくと、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが発生した場合に syslog と SNMP 通知がセカンダリ サーバーに転送されるようにするために、管理者が追加の作業を行わなければならない状況になることがあります。一般的な方法は、両方のサーバーにすべてのsyslogとトラップを転送するようにデバイスを設定することです。このためには通常、転送先をプライマリ サーバーとセカンダリ サーバーの両方を含む特定のサブネットまたは IP アドレス範囲に設定します。

この設定作業は、HA のセットアップと同時、つまりセカンダリ サーバーのインストール後からプライマリ サーバーでの HA の登録までの間に行う必要があります。これはフェールオーバーが発生する前に完了しておく必要があります。これにより、データが失われる可能性を解消または削減できます。仮想 IP アドレスを使用しない場合、セカンダリ サーバーのインストール手順は変更されません。ただし通常どおり、個別の IP アドレスを使用してプライマリ サーバーとセカンダリ サーバーをプロビジョニングする必要があります。

オペレーションセンターで HA を使用する場合、この回避策は使用できません。この場合、仮想 IP アドレスを有効にすることが必須条件となります（「オペレーション センター用の HA の有効化」を参照）。

関連トピック

HA での仮想 IP アドレッシングの使用 （8 ページ）
HA の導入計画 （10 ページ）
HA のネットワーク スループットに関する制限事項 （11 ページ）
キャンパス モデルの使用 （13 ページ）
リモート モデルの使用 （14 ページ）
オペレーション センター用の HA の有効化 （16 ページ）

自動フェールオーバーと手動フェールオーバーの違い

自動フェールオーバーを行うように HA を設定すると、ネットワーク管理者による HA の管理の必要性が減少します。また、セカンダリ サーバーが自動的に起動されるため、フェールオーバーの発生原因となった状況への対応に要する時間が削減されます。

ただし、ほとんどの場合は、システムで手動フェールオーバーを設定することが推奨されます。この推奨に従うことで、断続的なネットワークの停止に伴い Prime Infrastructure がセカンダリ サーバーに頻繁にフェールオーバーすることがなくなります。この状況が発生する可能性が最も高いのは、リモートモデルを使用して HA を導入する場合です。このモデルは、特に帯域幅と遅延の急激な変化による影響を受けます（「関連項目」の「HA の導入計画」および「HA のネットワーク スループットに関する制限事項」参照）。

フェールオーバー タイプが [自動（Automatic）] に設定されている場合に、ネットワーク接続がダウンするか、またはプライマリ サーバーとセカンダリ サーバー間のネットワーク リンクが到達不能になると、プライマリ サーバーとセカンダリ サーバーの両方が同時にアクティブになる可能性がわずかながらあります。これは「スプリット ブレーン状況」と呼ばれます。

この状況を防ぐため、プライマリ サーバーはセカンダリ サーバーがアクティブかどうかを常に確認します。ネットワーク接続またはリンクが復元され、プライマリ サーバーからセカンダリ サーバーに再び到達可能になると、プライマリ サーバーはセカンダリ サーバーの状態を確認します。セカンダリ サーバーの状態がアクティブな場合、プライマリ サーバーは自らダウンします。続いてユーザーがプライマリ サーバーへの標準の手動フェールバックを実行できます。

この状況が発生するのは、プライマリ HA サーバーで自動フェールオーバーが設定されている場合だけであることに注意してください。プライマリ サーバーで手動フェールオーバーを設定

することで、この状況が発生する可能性が排除されます。これが、手動フェールオーバー設定を推奨するもう 1 つの理由です。

大企業では特に、自動フェールオーバーは不適切です。特定の HA 導入環境で自動フェールオーバーを実行することになった場合、管理者はプライマリ サーバーまたはセカンダリ サーバーに新規に追加されたデータのいずれかを選択しなければならないことがあります。つまり、スプリットブレーンの状況が発生するたびにデータが失われる可能性があります。この問題に対処するには、「関連項目」の「スプリット ブレイン シナリオからの回復方法」を参照してください。

HA が適切に管理されるために、Prime Infrastructure 管理者に推奨されるのは、フェールオーバーまたはフェールバックを開始する前に、常に以下を含む HA 導入の全体的な状態を確認することです。

- プライマリ サーバーの現在の状態。
- セカンダリ サーバーの現在の状態。
- 2 台のサーバー間の現在の接続状態。

関連トピック

HA の導入計画 （10 ページ）
HA のネットワーク スループットに関する制限事項 （11 ページ）
フェールバックのトリガー方法 （38 ページ）
スプリット ブレイン シナリオからの回復方法 （50 ページ）
オペレーション センター用の HA の有効化 （16 ページ）

オペレーション センター用の HA の有効化

オペレーション センターには、Prime Infrastructure の高可用性（HA）フレームワークとの互換性があります。オペレーション センター用の HA は、プライマリおよびセカンダリオペレーション センター サーバーを設定すると簡単に有効化できます。この操作は、オペレーション センターを使用して管理する通常の Prime Infrastructure サーバー インスタンスに対して HA を実装する場合と同様です。

セカンダリ サーバーではオペレーション センターの追加ライセンスは必要ありません。オペレーションセンター用の HA は、手動および自動の両方のフェールオーバーをサポートしています。フェールオーバーの発生時には、セカンダリ オペレーション センター サーバーがアクティブになると、プライマリ オペレーション センター サーバーからから管理されているすべてのインスタンスが自動的にセカンダリ サーバーに継承されます。プライマリ オペレーション センター サーバーが新規であってもすでに稼働中のオペレーション センターであっても、プライマリで HA を有効化することができます。

オペレーション センター用の HA の有効化は必須ではありません。ただし、オペレーション センター用に HA を有効化するよう選択した場合、オペレーション センターでの HA 登録時に仮想 IP アドレッシングを有効にすることもできます。仮想 IP を使用するには、プライマリ サーバーとセカンダリ サーバーが同じサブネットにあることが必要です。

仮想 IP を使用してオペレーション センター用の HA をセットアップするには、次のワークフローに従ってください。

1. 両方のサーバーで使用する仮想 IP アドレスを決定します。詳細については、関連項目の「HA での仮想 IP アドレッシングの使用」と「ハイ アベイラビリティをセットアップする前に」を参照してください。
2. プライマリ オペレーション センター HA サーバーとして使用するサーバーに Prime Infrastructure をインストールします。

   オペレーション センターが有効な Prime Infrastructure サーバーがあり、このサーバーを HA を備えたプライマリ オペレーション センター サーバーとして使用する場合は、オペレーション センター インスタンスと、そのオペレーション センター サーバーが管理するすべての Prime Infrastructure インスタンスから、シングル サインオン（SSO）サーバーを削除します。この操作は **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [SSO サーバー（SSO Servers）]** を選択し、**[SSO サーバーを削除（Delete SSO Server(s)）]** コマンドを使用すると簡単にできます。
3. セカンダリ サーバーをインストールし、HA を使用できるよう設定します。詳細については、「関連項目」の「HA セカンダリ サーバーのインストール方法」を参照してください。
4. プライマリでセカンダリ サーバーを登録します。このとき、仮想 IP を有効化するよう指定し、選択した仮想 IP アドレスを入力します。サーバーからログアウトし、仮想 IP アドレスでもう一度ログインます。詳細については、「関連項目」の「プライマリ サーバーでの HA の登録方法」を参照してください。
5. 新しいプライマリ HA サーバーの場合：オペレーション センター ライセンス ファイルをプライマリ サーバーに適用して、オペレーション センターに変換します。詳細については、「オペレーション センター ライセンスのアクティブ化」を参照してください。
6. プライマリ サーバーで仮想 IP アドレスを SSO サーバーとしてセットアップします。このとき、仮想 IP アドレスを SSO サーバーの IP アドレスとして指定します。詳細については、「関連項目」の「オペレーション センターの SSO を有効にする」を参照してください。

（注） 既定では、TOFU はプライマリ サーバーで有効になっており、プライマリまたはセカンダリに CA 証明書が展開されていない場合は、フェールオーバー後に PI インスタンスとセカンダリ サーバーから仮想 IP TOFU を削除します。フェールバック後、プライマリ サーバーで同じ操作を繰り返します。SSO（プライマリ）クライアントサーバーから仮想 IP の TOFU を削除するには、次の操作を行います。

```
ncs certvalidation tofu-certs deletecert host <virtual ip>
```

7. プライマリ オペレーション センター サーバーが管理する Prime Infrastructure のすべてのインスタンスで、仮想 IP SSO サーバーの設定を繰り返します。古い SSO 構成が削除されていること確認し、PI サーバーを独自の IP で起動します。
8. すべての Prime Infrastructure インスタンスからログアウトしてから、仮想 IP アドレスをオペレーション センター IP として使用してオペレーション センター インスタンスにログインします。
9. 新しいプライマリ HA サーバーの場合：「関連項目」の「オペレーション センターに Cisco Prime Infrastructure インスタンスを追加する」の説明に従って、Prime Infrastructure インスタンスをオペレーション センター サーバーに追加します。

詳細については、「関連項目」の「オペレーションセンターライセンスのアクティブ化」を参照してください。

（注） 管理対象サーバーと SSO 設定の両方で、ホスト名または IP アドレスを統一して使用することを推奨します。IP アドレスとホスト名の両方を含めると、OPC から管理対象 PI への相互起動時に SSO で予期しない動作が発生する可能性があります。

仮想 IP を使用せずにオペレーション センター用の HA をセットアップするには、次のワークフローに従ってください。

1. プライマリ オペレーション センター HA サーバーとして使用するサーバーに Prime Infrastructure をインストールします。

   オペレーションセンターが有効な Prime Infrastructure サーバーがあり、このサーバーを HA を備えたプライマリ オペレーション センター サーバーとして使用する場合は、オペレーション センター インスタンスと、そのオペレーション センター サーバーが管理するすべての Prime Infrastructure インスタンスから、シングル サインオン（SSO）サーバーを削除します。この操作は **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [SSO サーバー（SSO Servers）]** を選択し、**[SSO サーバーを削除（Delete SSO Server(s)）]** コマンドを使用すると簡単にできます。

2. セカンダリ サーバーをインストールし、HA を使用できるよう設定します。詳細については、「関連項目」の「HA セカンダリ サーバーのインストール方法」を参照してください。
3. プライマリ上でセカンダリ サーバーを登録します。
4. 新しいプライマリ HA サーバーの場合：オペレーション センター ライセンス ファイルをプライマリ サーバーに適用して、オペレーション センターに変換します。詳細については、「オペレーション センター ライセンスのアクティブ化」を参照してください。
5. プライマリ オペレーション センター サーバーによって管理される Prime Infrastructure のすべてのインスタンスに対して、プライマリ サーバー IP アドレスのセットアップを繰り返します。
6. すべての Prime Infrastructure インスタンスからログアウトして、プライマリ IP アドレスをオペレーション センター サーバー IP として使用してオペレーション センター インスタンスにログインします。
7. 新しいプライマリ HA サーバーの場合：「関連項目」の「オペレーションセンターに Cisco Prime Infrastructure インスタンスを追加する」の説明に従って、Prime Infrastructure インスタンスをオペレーション センター サーバーに追加します。

   詳細については、「関連項目」の「オペレーションセンターライセンスのアクティブ化」を参照してください。

関連トピック

HA での仮想 IP アドレッシングの使用 （8 ページ）
ハイ アベイラビリティをセットアップする前に （19 ページ）
HA セカンダリ サーバーのインストール方法 （21 ページ）

プライマリ サーバーでの HA の登録方法 （22 ページ）
オペレーション センター ライセンスのアクティブ化
Cisco Prime Infrastructure インスタンスをオペレーション センターに追加する

ハイ アベイラビリティのセットアップ

Prime Infrastructure で HA 機能を使用するには、以下の作業を行う必要があります。

1. HA を有効にするために必要な情報と設定が揃っていることを確認します。詳細については、「関連項目」の「ハイ アベイラビリティをセットアップする前に」を参照してください。
2. 2 台目の Prime Infrastructure サーバーをインストールし、セカンダリ HA サーバーとして機能するように設定します。詳細については、「HA セカンダリ サーバーのインストール方法」を参照してください。
3. プライマリ サーバーでハイ アベイラビリティ モードを設定します。このとき、インストールしたセカンダリ サーバーを HA フォールバック サーバーとして指定します。詳細については、「プライマリ サーバー上での HA の登録方法」を参照してください。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
HA の導入計画 （10 ページ）
オペレーション センター用の HA の有効化 （16 ページ）
ハイ アベイラビリティをセットアップする前に （19 ページ）
HA セカンダリ サーバーのインストール方法 （21 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
HA 登録中の動作 （27 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法 （31 ページ）
ハイ アベイラビリティのモニター （36 ページ）
ヘルス モニター Web ページへのアクセス （37 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

ハイ アベイラビリティをセットアップする前に

セットアップの前に、以下のものが必要です。

- Prime Infrastructure インストール ソフトウェア。HA セカンダリ サーバーを作成するには、このソフトウェアを使用します。このソフトウェアのバージョンは、プライマリ サーバーにインストールされている Prime Infrastructure のバージョンと一致していなければなりません。プライマリ サーバー ソフトウェアの現在のバージョンを確認するには、CLI **show version** コマンドを使用します。
- プライマリ サーバーにパッチが適用されている場合は、セカンダリ サーバーにも同じレベルのパッチを適用する必要があります。[管理（Administration）]>[ランセンスおよびソ

フトウェアアップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）] を選択すると、プライマリ サーバーに適用されているパッチの一覧が表示されます。ハイ アベイラビリティのセットアップ後に「ペアリング済みハイ アベイラビリティ サーバーのパッチ適用方法」の手順に従い、セカンダリ サーバーにプライマリ サーバーと同じレベルのパッチを適用します。

- プライマリ サーバーの要件を満たすか、それを上回るハードウェアおよびソフトウェア仕様を備えたセカンダリ サーバー。たとえば、プライマリ サーバーが Prime Infrastructure の標準サイズの OVA としてインストールされている場合、セカンダリ サーバーも標準サーバーとしてインストールする必要があります。この場合、セカンダリ サーバーは、『Cisco Prime Infastructure Quick Start Guide』に記載されている標準サイズのサーバーのすべての要件を満たすか、それを上回っていなければなりません。
- セカンダリ サーバーの IP アドレスまたはホスト名。プライマリ サーバーで HA を設定する際に必要になります。
- 仮想 IP アドレッシングを使用する場合：両方の HA サーバーで仮想 IP として使用する仮想 IPv4 および IPv6 アドレス。仮想 IP 機能を使用する場合のみ必須となります（「関連項目」の「HA での仮想 IP アドレッシングの使用」を参照）。仮想 IP アドレッシングを使用するには、両方の HA サーバーが同一サブネット上にあることが必要です。オペレーション センターで HA を使用するには、仮想 IP アドレッシングを使用する必要があります（「関連項目」の「オペレーション センター用の HA の有効化」を参照）。
- 任意の長さの認証キー。小文字の英字、大文字の英字、数字、および特殊文字のうち、少なくとも 3 種類の文字が含まれている必要があります。セカンダリ サーバーをインストールするときに、この認証キーを入力します。HA の実装では、このキーを使用して、プライマリ サーバーとセカンダリ サーバー間の通信を認証します。管理者は、プライマリ サーバーに HA を設定する際や、HA 実装のモニターおよび問題のトラブルシューティングを行うためにセカンダリ サーバーの Health Monitor ページにログオンする際にも、このキーを使用します。
- プライマリ サーバーに対して管理者権限を持つ Prime Infrastructure ユーザー ID。
- HA 状態変更の通知先として設定できる、有効なメール アドレス。Prime Infrastructure は、HA 登録、障害、フェールオーバーおよびフェールバックが発生すると、状態変更を通知する電子メールを送信します。
- 許容可能な結果の場合：プライマリ サーバーとセカンダリ サーバーの間のリンクにおいて、220 ミリ秒以下の遅延と 86 Mbps 以上の正味スループット。少なくともこのリンク品質を提供できなければ、データ レプリケーションの妨げとなり、HA 障害が発生する可能性があります。許容可能なパフォーマンス要件の範囲のアドバイスについては、「HA のネットワーク スループットに関する制限事項」を参照してください。
- プライマリ サーバーとセカンダリ サーバーの間にファイアウォールを設定する場合は、ファイアウォールが以下のポートで着信および発信 TCP/UDP を許可するようにしてください。
  - 8082：ヘルス モニター プロセスでハートビート メッセージを交換するために使用されます。
  - 1522：Oracle でデータを同期するために使用されます。

- 8085：ユーザーがハイ アベイラビリティの準備状況テストを実行すると、プライマリ サーバーとセカンダリ サーバー間のネットワーク帯域幅速度を確認するためにヘルス モニター プロセスで使用されます

- Prime Infrastructure の HA 実装とともにオペレーション センターを使用する予定がある場合：HA 対応の Prime Infrastructure サーバーのすべて（プライマリとセカンダリの両方）がホスト名を完全に解決していることを確認してください。

  詳細については、『Cisco Prime Infastructure Quick Start Guide』を参照してください。

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法（31 ページ）
HA での仮想 IP アドレッシングの使用 （8 ページ）
オペレーション センター用の HA の有効化 （16 ページ）
HA のネットワーク スループットに関する制限事項 （11 ページ）

HA セカンダリ サーバーのインストール方法

プライマリ サーバーにパッチが適用されている場合は、セカンダリ サーバーのインストール後、プライマリ サーバーで HA を登録する前に、同じパッチをセカンダリ サーバーにも必ず適用してください。

手順を開始する前に、必ず認証キーを決定しておいてください（「関連項目」の「ハイ アベイラビリティをセットアップする前に」参照）。

ステップ 1 プライマリ サーバーの場合と同じように、セカンダリ サーバーへの Prime Infrastructure サーバー ソフトウェアのインストールを開始します。サーバーのインストール手順については、『Cisco Prime Infrastructure Quick Start Guide』を参照してください。

ステップ 2 インストール中に、以下のプロンプトが出されます。

Will this server be used as a secondary for HA? (yes/no)

プロンプトで **yes** と入力します。

ステップ 3 次に、以下のように HA 認証キーの入力を求めるプロンプトが出されます。

Enter Authentication Key:

プロンプトで認証キーを入力します。確認プロンプトでパスワードを再入力します。

ステップ 4 セカンダリ サーバーのインストールが完了したら、以下の作業を行います。

a) 両方のサーバーで CLI **show version** コマンドを使用して、バージョンおよびパッチ レベルが同じであることを確認します（「Prime Infrastructure のバージョンおよびパッチ ステータスの確認」を参照）。

b) ncs status コマンドを実行して、すべてのプロセスが起動され、セカンダリ サーバーで実行中であることを確認します（「Prime Infrastructure サーバー ステータスの確認」を参照）。

c) プライマリ サーバーで HA を登録します（「プライマリ サーバーでの HA の登録方法」を参照）。

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）
ハイ アベイラビリティをセットアップする前に （19 ページ）
Prime Infrastructure のバージョンとパッチ ステータスの確認
Prime Infrastructure サーバーのステータスの確認
プライマリ サーバーでの HA の登録方法 （22 ページ）

プライマリ サーバーでの HA の登録方法

HA を有効にするには、プライマリ サーバーに HA を登録する必要があります。プライマリ サーバーが HA コンフィギュレーションに参加するために、サーバーのインストール中に必要となる設定はありません。プライマリ サーバーで必要な情報は次の情報のみです。

- インストールと設定が完了しているセカンダリ HA サーバーの IP アドレスまたはホスト名（「関連項目」の「HA セカンダリ サーバーのインストール方法」を参照）。
- セカンダリ サーバーのインストール時に設定した認証キー。
- 通知の送信先となる 1 つ以上の電子メール アドレス。
- フェールオーバー タイプと自動フェールオーバー（「自動フェールオーバーと手動フェールオーバーの違い」を参照）。

仮想 IP アドレッシングを使用する場合（「HA での仮想 IP アドレッシングの使用」を参照）、次の作業も必要となります。

- [仮想 IP の有効化（Enable Virtual IP）] チェックボックスを選択します。
- プライマリおよびセカンダリ HA サーバーで共有する IPv4 仮想 IP アドレスを指定します。IPv6 仮想 IP アドレスも指定できますが、これは必須ではありません。

次の手順では、プライマリ サーバーに HA を登録する方法について説明します。HA を再登録する場合にも、以下と同じ手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Prime Infrastructure にログインします。

ステップ 2 メニューから、**[管理（Administration）]**>**[設定（Settings）]**>**[ハイ アベイラビリティ（High Availability）]** の順に選択します。Prime Infrastructure に [HA ステータス（HA status）] ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択し、次のフィールドに入力します。

1. [セカンダリ サーバー（Secondary Server）]：セカンダリ サーバーの IP アドレスまたはホスト名を入力します。
2. [認証キー（Authentication Key）]：セカンダリ サーバーのインストール中に設定したパスワードを認証キーとして入力します。

3. [電子メール アドレス（Email Address）]：HA の状態変更に関する通知の送信先アドレス（またはコンマで区切ったアドレスのリスト）を入力します。[メール サーバー設定（Mail Server Configuration）] ページで電子メール通知をすでに設定している場合（「電子メール サーバー設定の構成」参照）、ここに入力するメール アドレスは、メール サーバーですでに設定されているアドレスのリストに追加されます。
4. [フェールオーバー タイプ（Failover Type）]：[手動（Manual）] または [自動（Automatic）] を選択します。[手動（Manual）] を選択することが推奨されます。

ステップ 4 仮想 IP 機能を使用する場合：[仮想 IP の有効化（Enable Virtual IP）] チェックボックスをオンにし、追加フィールドに次のように入力します。

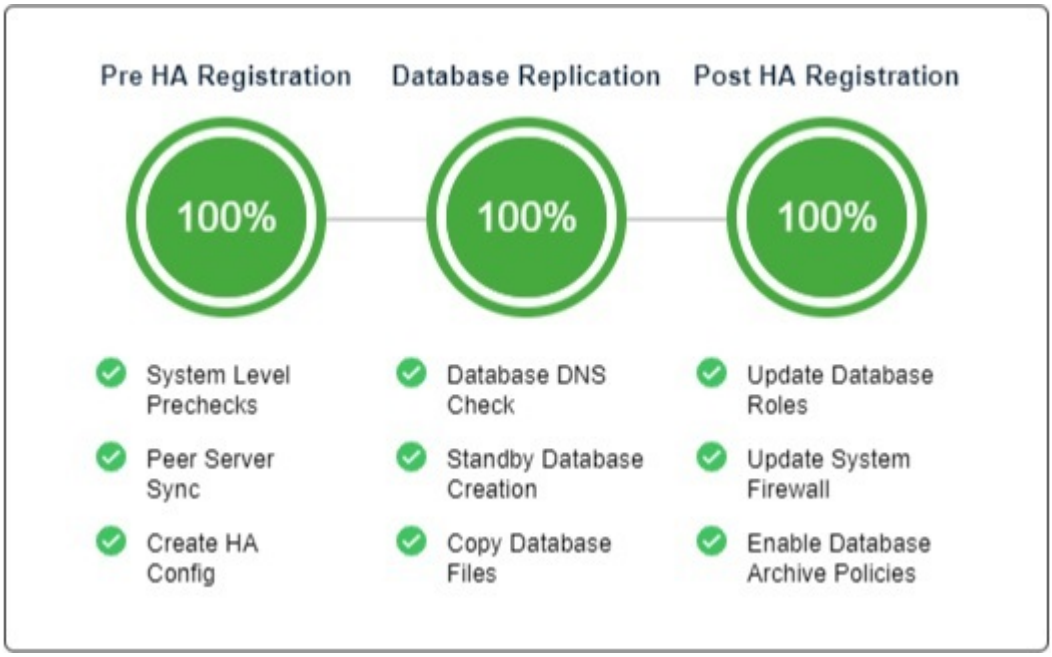
1. [IPV4 仮想 IP（IPV4 Virtual IP）]：両方の HA サーバーに使用する仮想 IPv4 アドレスを入力します。
2. [IPV6 Virtual IP]：（オプション）両方の HA サーバーに使用する仮想 IPv6 アドレスを入力します。

両方のサーバーが同一サブネット上にない場合は、仮想 IP アドレッシングは機能**しない**ことに注意してください。IPV6 アドレス ブロック fe80 は、リンクローカル ユニキャスト アドレッシング用に予約されているため使用しないでください。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックし、HA 関連の環境パラメータが設定を行える状態になっているか確認します。

詳細については、「HA 登録/設定の準備状況の確認」を参照してください。

ステップ 6 [登録（Register）] をクリックしてマイルストーン進行状況バーを表示し、以下に示すように、プレ HA 登録、データベース レプリケーション、およびポスト HA 登録が 100% 完了していることを確認します。Prime Infrastructure により HA 登録プロセスが開始されます。登録が正常に完了すると、[コンフィギュレーション モード（Configuration Mode）] に、[プライマリ アクティブ（Primary Active）] という値が表示されます。



詳細については、電子メール サーバー設定の構成を参照してください。

関連トピック

HA セカンダリ サーバーのインストール方法 （21 ページ）
自動フェールオーバーと手動フェールオーバーの違い （15 ページ）
HA での仮想 IP アドレッシングの使用 （8 ページ）
ハイ アベイラビリティをセットアップする前に （19 ページ）
HA 登録中の動作 （27 ページ）
ハイ アベイラビリティのセットアップ （19 ページ）
HA の登録/設定の準備状況の確認 （24 ページ）

HA の登録/設定の準備状況の確認

HA 登録時に、HA に関連する他の環境パラメータ（システム仕様、ネットワーク構成、サーバー間の帯域幅など）によって HA 設定が決定されます。

約 15 のチェックがシステム内で実行されて、エラーや障害が発生することなく HA 設定が完了したことが確認されます。準備状況の確認機能を実行すると、チェックリストの名前および対応するステータスが、該当する場合は推奨事項とともに表示されます。

HA 設定の準備状況を確認するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Prime Infrastructure にログインします。

ステップ 2 メニューから、**[管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]** の順に選択します。Prime Infrastructure に [HA ステータス（HA status）] ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択します。

ステップ 4 [セカンダリ サーバー（Secondary Server）] フィールドにセカンダリ サーバーの IP アドレスを入力し、[認証キー（Authentication Key）] フィールドのセカンダリの認証キーを入力します。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックします。

ポップアップ ウィンドウが開き、システム仕様およびその他のパラメータが表示されます。画面には、チェックリスト項目の名前、ステータス、影響、推奨事項の詳細が示されます。

その下に、準備状況の確認に使用されたチェックリストのテスト名と説明のリストが表示されます。

表 *1:* チェックリストの名前と説明

チェックリストのテスト名	テストの説明
システム - CPU 数の確認（SYSTEM - Check CPU Count）	プライマリサーバーとセカンダリサーバーの CPU 数を検証します。 プライマリ サーバーの CPU 数は、セカンダリ サーバーの CPU 数以下の場合があります。

データベース - リスナーのステータス（DATABASE - LISTENER STATUS）	データベースのリスナーがプライマリ サーバーとセカンダリ サーバーの両方で稼働中であるかどうかを確認します。 障害が発生した場合、テストが再起動されてステータスが報告されます。 wcs インスタンスのすべてが oracle「listener.ora」ファイル内にあるかどうかを確認します。このテストはプライマリ サーバーとセカンダリ サーバーの両方で実行されます。
データベース - メモリターゲットの確認（DATABASE - CHECK MEMORY TARGET）	HA セットアップの「/dev/shm」データベースのメモリ ターゲット サイズを確認します。
データベース - リスナー設定ファイルの破損確認（DATABASE - CHECK LISTENER CONFIG CORRUPTION）	すべてのデータベース インスタンスがデータベース リスナー設定に存在することを確認します。 このテストはプライマリ サーバーとセカンダリ サーバーの両方で実行されます。
システム - ヘルス モニターのステータス（SYSTEM - HEALTH MONITOR STATUS）	ヘルス モニター プロセスがプライマリ サーバーとセカンダリ サーバーの両方で実行されていることを確認します。
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリ サーバーとセカンダリ サーバーの両方でディスク IOPS を検証します。 必要な最小ディスク IOPS は 200 Mbps です。
ネットワーク - データベース ポートの開閉についてファイアウォールの確認（NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY）	データベース ポート 1522 がシステム ファイアウォールでオープンになっていることを確認します。 このポートが無効になっていると、テストは iptables リストで 1522 の権限を付与します。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	プライマリ サーバーとセカンダリ サーバーの両方で eth0 インターフェイス速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - ネットワーク帯域幅速度の確認（NETWORK - CHECK NETWORK BANDWIDTH SPEED）	プライマリ サーバーとセカンダリ サーバーの両方でネットワーク帯域幅速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバーの間でデータを送信することによってネットワーク帯域幅を測定します。

データベース - オンラインステータスの確認（DATABASE - CHECK ONLINE STATUS）	プライマリ サーバーとセカンダリ サーバーの両方でデータベース ファイルのステータスがオンラインでアクセス可能であることを確認します。
データベース - TNS 設定ファイルの破損確認（DATABASE - CHECK TNS CONFIG CORRUPTION）	プライマリ サーバーとセカンダリ サーバーの両方で tnsping が成功するかどうかを検証します。
データベース - TNS 到達可能性のステータス（DATABASE - TNS REACHABILITY STATUS）	wcs インスタンスのすべてが oracle「listener.ora」ファイル内にあるかどうかを確認します。 このテストはプライマリ サーバーとセカンダリ サーバーの両方で実行されます。
データベース - スタンバイデータベースインスタンスの検証（DATABASE - VALIDATE STANDBY DATABASE INSTANCE）	スタンバイ データベース インスタンス（stbywcs）がプライマリ サーバーとセカンダリ サーバーの両方で使用できるかどうかを検証します。
システム - RAM サイズの確認（SYSTEM - CHECK RAM SIZE）	プライマリ サーバーのディスク サイズがセカンダリ サーバーのディスク サイズ以下かどうかを確認します。
システム - サーバーへの ping 確認（SYSTEM - CHECK SERVER PING REACHABILITY）	プライマリ サーバーがリモート（セカンダリ）サーバーとの ping チェックを実行できることを確認します。

ステップ 6 すべてのパラメータのチェックが完了したら、パラメータのステータスを確認し、[クリア（Clear）] をクリックしてウィンドウを閉じます。

（注） 準備状況の確認中の検証フェールバックおよびフェールオーバー イベントは [アラームおよびイベント（Alarms and Events ）] ページに送信されますが、登録失敗イベントは [アラームおよびイベント（Alarms and Events ）] ページに表示されません。

ハイ アベイラビリティ ステータスの確認

Prime Infrastructure サーバー上で有効になっているハイ アベイラビリティのステータスを確認できます。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法を参照）。

ステップ 2 次のコマンドを入力して、Prime Infrastructure HA プロセスの現在のステータスを表示します。

PIServer/admin# **ncs ha status**

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）

HA 登録中の動作

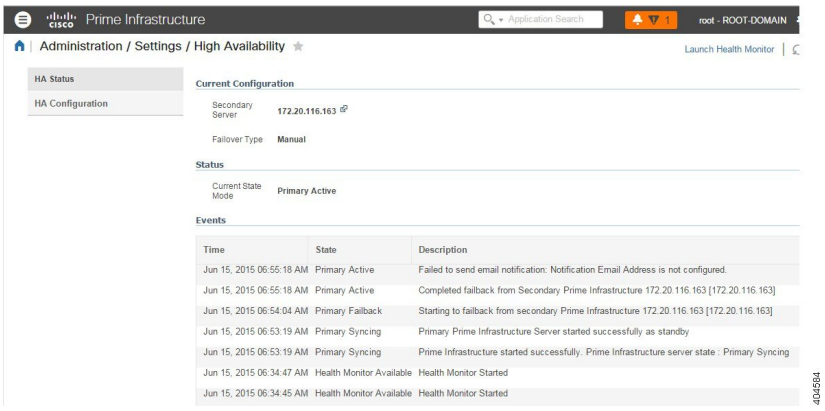
[HA 設定（HA Configuration）] ページで設定情報の入力を完了して [保存（Save）] をクリックすると、プライマリおよびセカンダリ HA サーバーが互いを登録し、プライマリ サーバーからセカンダリ サーバーにすべてのデータベースおよび構成データをコピーするプロセスが開始されます。

コピーが完了するまでの時間は、複製するデータベースおよび構成データの量と、2 台のサーバー間のネットワーク リンクで使用可能な帯域幅によって異なります。データの量が多かったり、リンクの速度が遅かったりすると、レプリケーションにもそれだけ時間がかかります。比較的新しいサーバー（数日しか稼動していないサーバー）の場合、デバイス数が 100 で、リンク速度が 1 Gbps だとすると、コピーには約 25 分かかります。

HA の登録中に、プライマリ サーバーとセカンダリ サーバーの状態は以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：HA not Configured	元の状態：HA not Configured
次の状態：HA Initializing	次の状態：HA Initializing
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

これらの状態変更は、プライマリ サーバーの [HA Status] ページまたは 2 台のサーバーのいずれかの Health Monitor Web ページで確認できます。[HA ステータス（HA Status）] ページを使用している場合は、[更新（Refresh）] をクリックすると、進行状況が表示されます。データが完全に同期すると、次の図に示すように、[HA ステータス（HA Status）] ページが更新され、現在の状態として [プライマリ アクティブ（Primary Active）] が表示されます。



登録が開始されると、Prime Infrastructure により、プライマリおよびセカンダリ HA サーバー間の同期が開始されます。同期によってユーザーアクティビティに影響が及ぶことはありませんが、同期が完了するまでは、ユーザーがシステム応答速度が低下したと感じる場合がありま

す。同期の所要時間は、データベースの合計サイズによって決まります。同期は、RMANおよびData Guard Brokerのプロセスによって Oracle データベース レベルで処理されます。同期中、ユーザーまたはシステム関連のアクティビティの実行への影響はありません。

登録時に、Prime Infrastructure はセカンダリ サーバーに完全なデータベースを複製します。セカンダリ サーバー上のすべてのプロセスが実行されますが、サーバー自体はパッシブ モードになります。セカンダリ サーバーが「セカンダリ同期中（Secondary Syncing）」状態のときに、Prime Infrastructure の CLI コマンド **ncs status** をセカンダリ サーバー上で実行すると、コマンド出力にはすべてのプロセスが実行中として表示されます。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
HA の導入計画 （10 ページ）
ハイ アベイラビリティのセットアップ （19 ページ）

HA サーバーにパッチを適用する方法

状況に応じて、次の方法のいずれかでHA サーバーの UBF パッチのダウンロードとインストールを行います。

- 現在ペアリングされていない HA サーバーにパッチをインストールします。Prime Infrastructure の HA が設定されていない場合は、この方法が推奨されます。
- 手動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。HA がすでに設定されている場合はこの方法が推奨されます。
- 自動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。

それぞれの方法の詳細については、「関連項目」を参照してください。

関連トピック

新しい HA サーバーへのパッチ適用方法 （28 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法（31 ページ）
自動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチを適用する方法 （33 ページ）

新しい HA サーバーへのパッチ適用方法

新しい Prime Infrastructure ハイ アベイラビリティ（HA）実装をセットアップするが、新しいサーバーが同一パッチ レベルではない場合には、次の手順に従って両方のサーバーにパッチをインストールし、同じパッチ レベルにします。

ステップ 1 パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco Prime Infrastructure 用ソフトウェア パッチのリストにアクセスします（「関連項目」を参照）。
b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[管理（Administration）] > [ランセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（Upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
h) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
i) プライマリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 2 セカンダリ サーバーに同じパッチをインストールします。

a) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

（注） ユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

（注） HM Web ページに表示されるセカンダリ サーバーの状態が [セカンダリ同期中（Secondary Syncing）] となっていることを確認します。

b) ユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。
c) HM Web ページの [Software Update] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[Login] を再びクリックします。
d) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
h) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。

i) セカンダリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 3 両方のサーバーのパッチ ステータスが同一であることを次のように確認します。

a) 上記のステップ 1 と同じ方法でプライマリ サーバーにログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

b) 上記のステップ 2 と同じ方法でセカンダリ サーバーのヘルス モニター Web ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

ステップ 4 サーバーを登録します。

詳細については、「Cisco Prime Infrastructure 用ソフトウェア パッチのリスト」、「Prime Infrastructure の再起動」および「Prime Infrastructure サーバー ステータスの確認」を参照してください。

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
HA サーバーにパッチを適用する方法 （28 ページ）

ペアリング済み HA サーバーへのパッチ適用方法

現在の Prime Infrastructure 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに適用する必要がある新しいパッチがある場合は、次の手順を実行します。

ペアリング済み HA サーバーへのパッチの適用はサポートされていません。HA が設定されている状態では Prime Infrastructure サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されます。そのため、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。

1. 「GUI での HA の削除」の手順（「関連項目」を参照）に従って、プライマリ サーバーとセカンダリ サーバーとの接続を切断します。
2. 「新しい HA サーバーのパッチ適用方法」の手順に従ってパッチを適用します。
3. HA の設定を復元するには、「ハイ アベイラビリティのセットアップ」の手順に従ってください。

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）
ハイ アベイラビリティ ステータスの確認 （26 ページ）
GUI での HA の削除 （56 ページ）
新しい HA サーバーへのパッチ適用方法 （28 ページ）

手動フェールオーバー用に設定されているペアリング済みHAサーバーのパッチ適用方法

現在の Prime Infrastructure 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに適用する必要がある新しいパッチがある場合は、次の手順を実行します。

パッチのインストールは、[プライマリ アクティブ（Primary Active）] 状態のプライマリ サーバー、および[セカンダリ同期中（Secondary Syncing）] 状態のセカンダリ サーバーで開始する必要があります。

手動フェールオーバー用に設定されているプライマリおよびセカンダリ HA サーバーのパッチ適用は約 30 分かかります。フェールオーバーとフェールバックは必要ではありません。プライマリ HA サーバーとセカンダリ HA サーバーにパッチを適用するには、約 30 分かかります。プライマリ パッチのインストール再起動時のダウンタイムは 15 ～ 20 分です。

場合によっては、HA が設定されている状態では Prime Infrastructure サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されることがあります。その場合、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。この場合、この手順のステップを使用できません。代わりに、次の手順に従います。

1. 「GUI での HA の削除」の手順（「関連項目」を参照）に従って、プライマリ サーバーとセカンダリ サーバーとの接続を切断します。
2. 「新しい HA サーバーのパッチ適用方法」の手順に従ってパッチを適用します。

（注） HA が有効になっている場合は、ユーザー名と認証キーの入力が求められます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

3. HA の設定を復元するには、「ハイ アベイラビリティのセットアップ」の手順に従ってください。

ステップ 1 HA 実装が有効になっていて、更新できる状態であることを確認します。

a) 管理者特権を持つ ID を使用して、プライマリ サーバーにログインします。

b) [Administration] > [Settings] > [High Availability] を選択します。[HA Status] ページに表示されるプライマリ サーバーの状態が [Primary Active] になっているはずです。

c) [HA 設定（HA Configuration）] を選択します。現在の [Configuration Mode] が、[HA Enabled] になります。パッチのインストール中にフェールオーバー タイプを [manual] に設定することを推奨します。

d) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

e) HM Web ページに表示されるセカンダリ サーバーの状態が [セカンダリ同期中（Secondary Syncing）] となっていることを確認します。

ステップ 2 HA を有効にしたときに入力したユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

ステップ 3 UBF パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco Prime Infrastructure 用ソフトウェア パッチのリストにアクセスします（「関連項目」を参照）。
b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[管理（Administration）] > [ランセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（Upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
h) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
i) プライマリ サーバーの再起動が完了した後、[管理（Administration）] > [設定（Settings）] > [ハイ アベイラビリティ（High Availability）] を選択します。[HA ステータス（HA Status）] ページに表示されるプライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）] です。
j) [ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、パッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 4 プライマリ サーバーにパッチを適用したら、同じパッチをセカンダリ サーバーにもインストールします。

a) セカンダリ サーバーの HM Web ページにアクセスし、必要に応じてログインします。
b) HM Web ページの [Software Update] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[Login] を再びクリックします。
c) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。
d) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
e) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
f) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
g) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
h) セカンダリ サーバーが再起動したら、セカンダリ HM ページ（https://serverIP:8082）にログインして、HM Web ページに表示されているセカンダリ サーバーの状態が「セカンダリ同期中（Secondary Syncing）」であることを確認します。

i) [ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、パッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 5 サーバーが再起動したら、以下の手順でパッチのインストールを確認します。

a) 上記のステップ 2 と同じ方法でプライマリ サーバーにログインし、[ソフトウェアアップデート（Software Update）] ページにアクセスします。[Status of Updates] > [Update] タブの [Status] 列に、パッチのステータスが [Installed] と表示されている必要があります。

b) 上記のステップ 3 と同じ方法でセカンダリ サーバーの [Software Update] ページにアクセスします。[アップデートのステータス（Status of Updates）]>[アップデート（Updates）] タブの [ステータス（Status）] 列に、パッチのステータスが [インストール済み（Installed）] と表示されている必要があります。

詳細については、次を参照してください。

- Cisco Prime Infrastructure のソフトウェア パッチのリスト。
- Prime Infrastructure の起動
- Prime Infrastructure の停止
- Prime Infrastructure サーバーのステータスの確認

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）
ハイ アベイラビリティ ステータスの確認 （26 ページ）
GUI での HA の削除 （56 ページ）
新しい HA サーバーへのパッチ適用方法 （28 ページ）
自動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチを適用する方法 （33 ページ）

自動フェールオーバー用に設定されているペアリング済みHAサーバーのパッチを適用する方法

現在の Prime Infrastructure 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに適用する必要がある新しいパッチがある場合は、次の手順を実行します。

パッチのインストールは、[プライマリ アクティブ（Primary Active）] 状態のプライマリ サーバー、および [セカンダリ同期中（Secondary Syncing）] 状態のセカンダリ サーバーで開始する必要があります。

自動フェールオーバー用に設定されているプライマリおよびセカンダリ HA サーバーのパッチ適用は約 1 時間かかります。また、フェールオーバーとフェールバックの両方が必要です。フェールオーバーとフェイルバックによるダウンタイムは 10 ～ 15 分です。

場合によっては、HA が設定されている状態では Prime Infrastructure サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されることがあります。その場合、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。この場合、この手順のステップを使用できません。代わりに、次の手順に従います。

1. 「GUI での HA の削除」の手順（「関連項目」を参照）に従って、プライマリ サーバーとセカンダリ サーバーとの接続を切断します。
2. 「新しいHAサーバーへのパッチ適用方法」（「関連項目」を参照）の手順に従って、パッチを適用します。
3. HA の設定を復元するには、「ハイ アベイラビリティのセットアップ」（「関連項目」を参照）の手順に従ってください。

ステップ 1 HA 実装が有効になっていて、更新できる状態であることを確認します。

a) 管理者特権を持つ ID を使用して、プライマリ サーバーにログインします。
b) [Administration] > [Settings] > [High Availability] を選択します。[HA Status] ページに表示されるプライマリ サーバーの状態が [Primary Active] になっているはずです。
c) [HA 設定（HA Configuration）] を選択します。現在の [Configuration Mode] が、[HA Enabled] になります。
d) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

e) HA を有効にしたときに入力したユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。
f) HM Web ページに表示されるセカンダリ サーバーの状態が [セカンダリ同期中（Secondary Syncing）] となっていることを確認します。

ステップ 2 UBF パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco Prime Infrastructure 用ソフトウェア パッチのリストにアクセスします（「関連項目」を参照）。
b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[管理（Administration）] > [ランセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。

h) 警告ポップアップで、[はい（Yes）] をクリックします。フェールオーバーがトリガーされ、プライマリ サーバーが自動的に再起動します。フェールオーバーが完了するまでに 2 ～ 4 時間かかります。フェールオーバーが完了すると、セカンダリ サーバーは「セカンダリ アクティブ（Secondary Active）」状態になります。

i) プライマリ サーバーが再起動したら、**ncs status** コマンドを実行（「Prime Infrastructure サーバー ステータスの確認」を参照）して、プライマリ サーバーのプロセスが再開したことを確認します。続行する前に：プライマリ サーバーの HM Web ページにアクセスし、表示されたプライマリ サーバーの状態が「プライマリ同期中（Primary Synching）」であることを確認します。

ステップ 3 セカンダリ サーバーの HM Web ページを使用して、プライマリ サーバーにフェールバックします。

a) セカンダリ サーバーの HM Web ページにアクセスし、必要に応じてログインします。

b) [Failback] をクリックして、セカンダリ サーバーからプライマリ サーバーへのフェールバックを開始します。動作が完了するまで2～3分かかります。フェールバックが完了するとすぐに、セカンダリ サーバーは自動的にスタンバイ モードで再起動します。再起動が完了するまでに最大15分間かかります。そして、プライマリ サーバーと同期されます。

再起動の確認は、セカンダリ サーバーの HM Web ページにログインし、[Prime Infrastructure は正常に起動しました（Prime Infrastructure stopped successfully）]、および [Prime Infrastructure は正常に停止しました（Prime Infrastructure started successfully）] というメッセージを探すことで行えます。

フェールバックが完了した後、プライマリ サーバーの状態が「プライマリ アクティブ（Primary Active）」に変更されます。

c) 続行する前に：プライマリ サーバーとセカンダリ サーバーの両方で **ncs ha status** コマンドを実行します。プライマリ サーバーの状態が「プライマリ アクティブ（Primary Active）」に変わり、セカンダリ サーバーの状態が「セカンダリ同期中（Secondary Synching）」であることを確認します。

ステップ 4 フェールバックが完了したら、プライマリ サーバーに上記にログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスして、パッチのインストールを確認します（上記のステップ 2 と同様です）。[アップデートのステータス（Status of Updates）] > [アップデート（Update）] タブの [ステータス（Status）] 列に、パッチのステータスが [インストール済み（Installed）] と表示されている必要があります。

ステップ 5 プライマリ サーバーにパッチを適用したら、同じパッチをセカンダリ サーバーにもインストールします。

a) セカンダリ サーバーの HM Web ページにアクセスし、必要に応じてログインします。

b) HM Web ページの [Software Update] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[Login] を再びクリックします。

c) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。

d) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。

e) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。

f) パッチ ファイルを選択し、[インストール（Install）] をクリックします。

g) 警告ポップアップで、[はい（Yes）] をクリックします。サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。

h) セカンダリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

i) セカンダリ サーバーが再起動したら、セカンダリ HM ページにログインして、HM Web ページに表示されているセカンダリ サーバーの状態が「セカンダリ同期中（Secondary Syncing）」であることを確認します。

ステップ 6 サーバーが再起動したら、以下の手順でパッチのインストールを確認します。

a) 上記のステップ 2 と同じ方法でプライマリ サーバーにログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスします。[Status of Updates] > [Update] タブの [Status] 列に、パッチのステータスが [Installed] と表示されている必要があります。

b) 上記のステップ 5 と同じ方法でセカンダリ サーバーの [ソフトウェア アップデート（Software Update）] ページにアクセスします。[アップデートのステータス（Status of Updates）]>[アップデート（Updates）] タブの [ステータス（Status）] 列に、パッチのステータスが [インストール済み（Installed）] と表示されている必要があります。

詳細にういては、「Cisco Prime Infrastructure 用ソフトウェア パッチのリスト」、「Prime Infrastructure の停止」、「Prime Infrastructure の起動」および「Prime Infrastructure サーバー ステータスの確認」を参照してください。

関連トピック

ハイ アベイラビリティのセットアップ （19 ページ）
ハイ アベイラビリティ ステータスの確認 （26 ページ）
GUI での HA の削除 （56 ページ）
新しい HA サーバーへのパッチ適用方法 （28 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法 （31 ページ）

ハイ アベイラビリティのモニター

HA を設定し、それをプライマリ サーバー上で登録した後、HA とのやり取りでは、ほとんどの場合、サーバーの Health Monitor Web ページにアクセスし、フェールオーバーまたはフェールバックをトリガーして電子メールでの通知に応答することになります。これらのプロセスおよび複雑な応答を必要とする特別な状況について、次の「関連項目」で説明しています。

関連トピック

ヘルス モニター Web ページへのアクセス （37 ページ）
フェールオーバーのトリガー方法 （37 ページ）
フェールバックのトリガー方法 （38 ページ）
フェールオーバーの強制実行 （39 ページ）
その他の HA イベントに対する応答 （40 ページ）

ヘルス モニター Web ページへのアクセス

プライマリ サーバーとセカンダリ サーバーの Health Monitor Web ページにアクセスするには、ブラウザで次の URL を開きます。

https://**Server**:8082

ここで、**Server** は、Health Monitor Web ページを表示する対象のプライマリ サーバーまたはセカンダリ サーバーの IP アドレスまたはホスト名です。

（注） ユーザー名と認証キーの入力を求められます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

現在アクティブなサーバーのヘルス モニター Web ページにアクセスするには、Prime Infrastructure にログインして [管理（Administration）] > [設定（Settings）] > [ハイ アベイラビリティ（High Availability）] を選択し、[HA ステータス（HA Status）] ページの右上にある [ヘルス モニターの起動（Launch Health Monitor）] リンクをクリックします。

関連トピック

ハイ アベイラビリティのモニター （36 ページ）
フェールオーバーのトリガー方法 （37 ページ）
フェールバックのトリガー方法 （38 ページ）
フェールオーバーの強制実行 （39 ページ）

フェールオーバーのトリガー方法

フェールオーバーとは、プライマリ サーバーで検出された障害への対応として、セカンダリ サーバーをアクティブ化するプロセスのことです。

Health Monitor（HM）は、2 台のサーバー間で交換されるハートビート メッセージを使用して障害状態を検出します。プライマリ サーバーがセカンダリ サーバーから送信されるハートビート メッセージに 3 回連続して応答しない場合、プライマリ サーバーに障害が発生したと見なされます。ヘルス チェック中に、HM はアプリケーション プロセスのステータスおよびデータベースのヘルスもチェックします。これらのチェックに対して適切な応答がない場合は、アプリケーション プロセスやデータベースも障害が発生しているとして処理されます。

HA システムがプライマリ サーバーでのプロセス障害を検出してフェールオーバーを開始するまでには、約 10 秒から 15 秒かかります。ネットワークの問題によってセカンダリ サーバーがプライマリ サーバーに接続できない場合は、フェールオーバーを開始するまでに、さらに長い時間がかかることがあります。また、セカンダリ サーバーでのアプリケーション プロセスが完全に機能するようになるまでにも時間がかかることがあります。

HM は障害を検知するとすぐに、電子メールでの通知を送信します。この E メールには、障害ステータスに加え、セカンダリ サーバーの Health Monitor Web ページへのリンクも記載されます。

HA が自動フェールオーバーを行うよう設定されている場合は、セカンダリ サーバーが自動的にアクティブ化されるため、ユーザーが実行しなければならないアクションはありません。

HA が手動フェールオーバー用に設定されている場合は、以下の手順に従ってフェールオーバーをトリガーする必要があります。

フェールオーバーは、一時的なものであると見なす必要があります。障害が発生したプライマリ Prime Infrastructure インスタンスをできるだけ早く復旧して、フェールバックを再開する必要があります。

ステップ 1 電子メールでの通知に記載されている Web リンクを使用するか、または「Health Monitor Web ページへのアクセス」の手順に従って、セカンダリ サーバーの Health Monitor Web ページにアクセスします。

ステップ 2 [フェールオーバー（Failover）] ボタンをクリックしてフェールオーバーをトリガーします。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
フェールバックのトリガー方法 （38 ページ）
ハイ アベイラビリティのモニター （36 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
ヘルス モニター Web ページへのアクセス （37 ページ）

フェールバックのトリガー方法

フェールバックとは、オンライン状態に戻ったプライマリ サーバーをアクティブ化するプロセスのことです。また、このプロセスでは、アクティブ ステータスをセカンダリ サーバーからプライマリ サーバーに移して、セカンダリ サーバーでのアクティブなネットワーク モニタリング プロセスを停止します。

フェールバック中は、プロセスがセカンダリ サーバー上で再開される期間を除き、セカンダリ サーバーを使用できます。両方のサーバーの Health Monitor Web ページにアクセスして、フェールバックの進行状態をモニターすることができます。さらに、ユーザーはセカンダリ サーバーに接続して、通常のすべての機能を使用することもできます。ただし、その場合は以下の注意事項があります。

- フェールバックの進行中は、設定またはプロビジョニングのアクティビティを開始しないでください。
- フェールバックが正常に完了すると、セカンダリ サーバーがパッシブ（「セカンダリ同期中（Secondary Syncing）」）モードに移行して、制御がプライマリ サーバーに切り替わることに注意してください。このプロセス中は、しばらくの間、ユーザーが Prime Infrastructure にアクセスできなくなります。

フェールバックは常に、手動でトリガーする必要があります。それには、以下の手順に従います。

ステップ 1 電子メールでの通知に記載されているリンクを使用するか、または「Health Monitor Web ページへのアクセス」の手順に従って、セカンダリ サーバーの Health Monitor Web ページにアクセスします。

ステップ 2 [Failback] ボタンをクリックしてフェールバックをトリガーします。

セカンダリ サーバーは、フェールバック後に自動的にスタンバイ モードで再起動され、自動的にプライマリ サーバーと同期されます。プライマリ サーバーが Prime Infrastructure サーバーとして利用可能になります。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
フェールオーバーのトリガー方法 （37 ページ）
フェールオーバーの強制実行 （39 ページ）
ハイ アベイラビリティのモニター （36 ページ）
ヘルス モニター Web ページへのアクセス （37 ページ）

フェールオーバーの強制実行

強制フェールオーバーは、プライマリ サーバーが稼働している間に、セカンダリ サーバーをアクティブにするプロセスです。このオプションは、たとえば、HA セットアップは完全に機能しているかどうかをテストする場合に使用します。

強制フェールオーバーを使用できるのは、プライマリがアクティブで、セカンダリが「セカンダリ同期中（Secondary Syncing）」状態であり、すべてのプロセスが両方のサーバーで実行中の場合に限られます。プライマリ サーバーがダウンしている場合、強制フェールオーバーは無効になります。この状況では、通常のフェールオーバーのみが有効です。

強制フェールオーバーが完了すると、セカンダリ サーバーがアクティブになり、プライマリ サーバーは自動的にスタンバイ状態で再起動します。通常のフェイルバックをトリガーすると、元の通りプライマリ サーバーがアクティブになり、セカンダリ サーバーがスタンバイ状態になります。

ステップ 1 「ヘルス モニター Web ページへのアクセス」の手順に従って、セカンダリ サーバーのヘルス モニター Web ページにアクセスします。

ステップ 2 [強制フェールオーバー（Force Failover）] ボタンをクリックして強制フェールオーバーをトリガーします。強制フェールオーバーは 2 ～ 3 分で完了します。

関連トピック

ハイ アベイラビリティの仕組み （1 ページ）
フェールオーバーのトリガー方法 （37 ページ）
フェールバックのトリガー方法 （38 ページ）
ハイ アベイラビリティのモニター （36 ページ）

プライマリ サーバーでの HA の登録方法 （22 ページ）
ヘルス モニター Web ページへのアクセス （37 ページ）

その他の HA イベントに対する応答

HA 関連のすべてのイベントは、[HA ステータス（HA Status）] ページ、ヘルス モニター Web ページ、および Prime Infrastructure の [アラームおよびイベント（Alarms and Events）] ページに表示されます。ほとんどのイベントには、オペレータの応答は不要ですが、フェールオーバーおよびフェールバックのトリガーは例外です。「関連項目」で説明するように、複雑なイベントもいくつかあります。

関連トピック

HA 登録が失敗した場合 （40 ページ）
ネットワークがダウンしている場合（自動フェールオーバー） （41 ページ）
ネットワークがダウンしている場合（手動フェールオーバー） （42 ページ）
プロセスをリスタートできない場合（手動フェールオーバー） （45 ページ）
同期中にプライマリ サーバーが再起動した場合（手動フェールオーバー） （46 ページ）
同期中にセカンダリ サーバーが再起動した場合 （46 ページ）
HA サーバーが両方ともダウンしている場合 （47 ページ）
HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （48 ページ）
プライマリ MSE の交換 （78 ページ）
スプリット ブレイン シナリオからの回復方法 （50 ページ）

HA 登録が失敗した場合

HA 登録が失敗すると、サーバーごとの HA 状態が、（「HA 登録中の動作」で説明したように変更されるのではなく）以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：HA Initializing	元の状態：HA Initializing
次の状態：HA not Configured	次の状態：HA not Configured

HA 登録の失敗から回復するには、次の手順に従います。

ステップ 1 ping または他のツールを使用して、2 台の Prime Infrastructure サーバー間のネットワーク接続を確認します。プライマリ サーバーからセカンダリ サーバーに接続できること、その逆も可能であることを確認します。

ステップ 2 ゲートウェイ、サブネットマスク、仮想IPアドレス（設定されている場合）、サーバーのホスト名、DNS、NTP 設定がすべて正しいことを確認します。

ステップ 3 設定された DNS および NTP サーバーにプライマリ サーバーとセカンダリ サーバーから接続可能であること、そして DNS および NTP サーバーの両方が遅延や他のネットワーク固有の問題を伴うことなく応答していることを確認します。

ステップ 4 すべての Prime Infrastructure ライセンスが正しく設定されていることを確認します。

ステップ 5 接続または設定の問題を解決したら、関連トピックの「プライマリ サーバーでのハイ アベイラビリティの登録方法」の手順を再試行します。

関連トピック

その他の HA イベントに対する応答 （40 ページ）
HA 登録中の動作 （27 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）

ネットワークがダウンしている場合（自動フェールオーバー）

フェールオーバー タイプが [自動（Automatic）] に設定されている場合、2 台の Prime Infrastructure サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Lost Secondary	次の状態：Secondary Failover
次の状態：Primary Lost Secondary	次の状態：[セカンダリ アクティブ（Secondary Active）]

セカンダリ サーバーがアクティブであることを示す電子メール通知を受信します。

ステップ 1 2 台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出できるようになったら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Active
次の状態：Primary Failover	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （40 ページ）
フェールバックのトリガー方法 （38 ページ）

ネットワークがダウンしている場合（手動フェールオーバー）

フェールオーバー タイプが [手動（Manual）] に設定されている場合、2 台の Prime Infrastructure サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

各サーバーがもう一方のサーバーを失ったことを通知する電子メールを受信します。

ステップ 1 2 台のサーバー間のネットワーク接続を確認し、必要に応じて復元します。

ネットワーク接続が復元されると、次ように状態が遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Lost Primary
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は不要です。

ステップ 2 何らかの理由でネットワーク接続を復元できない場合は、セカンダリ サーバーの HM Web ページを使用して、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Lost Primary
次の状態：Primary Lost Secondary	次の状態：Secondary Failover
次の状態：Primary Failover	次の状態：Secondary Active

セカンダリ サーバーがアクティブになったことを通知する電子メールを受信します。

ステップ 3 2台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出したら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Active
次の状態：Primary Failover	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 4 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。

以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （40 ページ）
フェールバックのトリガー方法 （38 ページ）

プロセスを再開できない場合（自動フェールオーバー）

Prime Infrastructure のヘルス モニター プロセスは、失敗した Prime Infrastructure サーバー プロセスのリスタートを試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。

HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。現在設定されているフェールオーバー タイプが [automatic] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Uncertain	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Failover	次の状態：Secondary Failover
次の状態：Primary Failover	次の状態：Secondary Active

このプロセスが完了すると、セカンダリ サーバーがアクティブになったことを通知する電子メールでの通知を受信します。

ステップ 1 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、その状態は [Primary Syncing] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Failover	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Preparing for Failback	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （40 ページ）
フェールバックのトリガー方法 （38 ページ）

プロセスをリスタートできない場合（手動フェールオーバー）

Prime Infrastructure のヘルス モニター プロセスは、失敗した Prime Infrastructure サーバー プロセスのリスタートを試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。その場合、障害を通知する電子メールを受信します。現在設定されているフェールオーバー タイプが [Manual] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Uncertain	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

ステップ 1 セカンダリ サーバーで、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Uncertain	元の状態：Secondary Syncing
次の状態：Primary Failover	次の状態：Secondary Failover
次の状態：Primary Failover	次の状態：Secondary Active

ステップ 2 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、プライマリ サーバーの HA 状態は [Primary Syncing] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Failover	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Preparing for Failback	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 3 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （40 ページ）
フェールオーバーのトリガー方法 （37 ページ）
フェールバックのトリガー方法 （38 ページ）

同期中にプライマリ サーバーが再起動した場合（手動フェールオーバー）

セカンダリ サーバーとの同期中に Prime Infrastructure サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Alone	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

[Primary Alone] および [Primary Active] 状態への遷移は、プライマリ サーバーがオンライン状態に戻った直後に行われます。管理者による応答は必要ありません。

関連トピック

その他の HA イベントに対する応答 （40 ページ）

同期中にセカンダリ サーバーが再起動した場合

プライマリ サーバーとの同期中にセカンダリ Prime Infrastructure サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Lost Secondary	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は必要ありません。

関連トピック

その他の HA イベントに対する応答 （40 ページ）

HA サーバーが両方ともダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーが同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーおよびセカンダリ サーバー上で稼働する Prime Infrastructure のインスタンスを再起動します。何らかの理由でセカンダリ サーバーを再起動できなかった場合は、「関連項目」の「HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合」を参照してください。

ステップ 2 セカンダリ サーバーで Prime Infrastructure が稼働中になったら、セカンダリ サーバーの Health Monitor Web ページにアクセスします。セカンダリ サーバーの状態が [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] に遷移します。

ステップ 3 プライマリ サーバーと、プライマリ サーバー上で稼働する Prime Infrastructure のインスタンスを再起動します。Prime Infrastructure がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーと同期します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （48 ページ）
ヘルス モニター Web ページへのアクセス （37 ページ）
その他の HA イベントに対する応答 （40 ページ）

両方の HA サーバーの電源がダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーの電源が同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーとその上で稼働する Prime Infrastructure のインスタンスの電源をオンにします。

この時点では、プライマリに到達できないため、セカンダリ HA の再起動に失敗します。ただし、セカンダリ ヘルス モニター プロセスは動作し、エラーが表示されます。

ステップ 2 セカンダリ サーバーで Prime Infrastructure が稼働中になったら、セカンダリ サーバーの Health Monitor Web ページにアクセスします。セカンダリ サーバーの状態が [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] に遷移します。

ステップ 3 プライマリ サーバと、プライマリ サーバ上で稼働する Prime Infrastructure のインスタンスの電源をオンにします。

ステップ 4 Prime Infrastructure がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーと同期します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

ステップ 5 セカンダリ サーバーとその上で稼働する Prime Infrastructure のインスタンスを再起動します。この時点では、プロセスのすべてがセカンダリ サーバーで実行されているわけではないため、この操作が必要です。

何らかの理由でセカンダリ サーバを再起動できなかった場合は、「関連項目」の「HA サーバが両方ともダウンし、セカンダリ サーバが再起動しない場合」を参照してください。

ステップ 6 Prime Infrastructure がセカンダリ サーバーでの再起動を完了すると、すべてのプロセスが実行されているはずです。これを確認するには、ncs status コマンドを実行します（「関連項目」の「Prime Infrastructure サーバーのステータスの確認」を参照）。

関連トピック

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （48 ページ）
ヘルス モニター Web ページへのアクセス （37 ページ）
その他の HA イベントに対する応答 （40 ページ）
Prime Infrastructure サーバーのステータスの確認

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合

両方の HA サーバーが同時にダウンし、セカンダリ サーバーが再起動しない場合は、セカンダリ サーバーの交換または復元ができるまで、プライマリ サーバーをスタンドアロンとして使用するように、プライマリ サーバーから HA 設定を削除する必要があります。

以下の手順では、すでにセカンダリ サーバーの再起動を試み、再起動に失敗したものとしています。

ステップ 1 Prime Infrastructure のプライマリ インスタンスの再起動を試みます。少なくともプライマリ インスタンスの再起動が可能である場合は、HA 設定の削除が必要であることを示すエラー メッセージが表示されて再起動が中断されます。

ステップ 2 プライマリ Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法を参照）。

ステップ 3 次のコマンドを入力して、プライマリ サーバーの HA 設定を削除します。

PIServer/admin# **ncs ha remove**

ステップ 4 HA 設定を削除するかどうかを確認するメッセージが表示されます。確認要求に対して **Y** と応答します。

今度は、エラー メッセージなしで Prime Infrastructure プライマリ インスタンスの再起動が可能になり、これをスタンドアロンとして使用できるようになるはずです。

セカンダリ サーバーの復元または交換ができたら、「関連項目」の「プライマリ サーバーでのハイ アベイラビリティの登録方法」の手順に従って続行してください。

関連トピック

ヘルス モニター Web ページへのアクセス （37 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
CLI での HA の削除 （57 ページ）
その他の HA イベントに対する応答 （40 ページ）

プライマリ サーバーの交換方法

通常の状況下では、プライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）]、セカンダリ サーバーの状態は [セカンダリ同期中（Secondary Syncing）] です。プライマリ サーバで何らかの理由で障害が発生した場合、セカンダリ サーバへのフェールオーバーが自動または手動で行われます。

HA への完全なアクセスを復旧するには、新しいハードウェアを使用してプライマリ サーバをインストールする必要があることがあります。この場合、次の手順に従うことで、データを失うことなく新しいプライマリ サーバを起動できます。

ステップ 1 セカンダリ サーバーの状態が [セカンダリ アクティブ（Secondary Active）] であることを確認します。プライマリ サーバの [Failover Type] を [manual] に設定している場合は、セカンダリ サーバへのフェールオーバーを手動でトリガーします。

ステップ 2 交換する古いプライマリ サーバーがネットワークから切断していることを確認します。

ステップ 3 新しいプライマリ サーバーが使用可能な状態であることを確認します。これには、このプライマリ サーバがネットワークに接続されており、古いプライマリ サーバと同じサーバ IP、サブネット マスク、およびゲートウェイが割り当てられていることが含まれます。また、セカンダリ サーバーのインストール時に入力したものと同じ認証キーを入力する必要があります。

ステップ 4 プライマリサーバーとセカンダリサーバーが同じパッチ レベルであることを確認します。プライマリサーバーを置換する場合は、次の手順を実行する必要があります。

a) プライマリサーバーとセカンダリサーバーが TOFU モードであることを確認します。
b) セカンダリサーバー管理 CLI にログインします。
c) セカンダリサーバーの CLI で次のコマンドを実行します。
d) PIServer/admin# ncs certvalidation tofu-certs deletecert host <primaryserver's-hostname>

これは、プライマリサーバーとセカンダリサーバー間の通信を再確立するために必要です。

ステップ 5 セカンダリ サーバーから、新たにインストールしたプライマリ サーバーへのフェールバックをトリガーします。新しいプライマリ HA サーバーへのフェールバック中にはデータベースのフル コピーが実行されるため、使用可能な帯域幅とネットワーク遅延によってはこの処理の完了に時間がかかります（「関連項目」の「HA のネットワーク スループットに関する制限事項」を参照）。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：HA not configured	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

フェールオーバーのトリガー方法 （37 ページ）
フェールバックのトリガー方法 （38 ページ）
その他の HA イベントに対する応答 （40 ページ）
HA のネットワーク スループットに関する制限事項 （11 ページ）

スプリット ブレイン シナリオからの回復方法

「自動フェールオーバーと手動フェールオーバーの違い」（「関連項目」参照）で説明されているように、「スプリットブレーン状況」が発生する稀な状況では、データが失われる可能性が常にあります。この場合、以下の手順に従い、新しく追加されたデータをセカンダリに保存し、追加されたデータをプライマリには保存しないようにすることができます。

ステップ 1 ネットワークが起動し、セカンダリ サーバーが起動すると、プライマリ サーバーはスタンバイ データベースを使用して自動的に再起動します。プライマリ サーバーの HA ステータスはまず「プライマリ フェールオーバー（Primary Failover）」になり、その後「プライマリ同期中（Primary Syncing）」に変わります。これを確認するには、プライマリ サーバーのヘルス モニター Web ページにログオンします。

ステップ 2 プライマリ サーバーのステータスが「プライマリ同期中（Primary Syncing）」になった後、Web ブラウザを使用して、ユーザーがセカンダリ サーバーの Prime Infrastructure ページ（たとえば、https://x.x.x.x:443）にログインできることを確認します。確認が済むまで、手順を進めないでください。

ステップ 3 セカンダリ サーバーにアクセスできることが確認できたら、セカンダリ サーバーのヘルス モニター Web ページから、フェールバックを開始します（フェールバックのトリガー方法 （38 ページ）を参照）。プライマリ サーバーへのスイッチオーバーが完了するまで、セカンダリ サーバーでモニタリング アクティビティを続行できます。

詳細については、CLI を使用した Prime Infrastructure の再起動を参照してください。

関連トピック

自動フェールオーバーと手動フェールオーバーの違い （15 ページ）
CLI での HA の削除 （57 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）

データベースの同期の問題を解決する方法

データベースの同期の問題を解決するには、プライマリ サーバーが「プライマリ アクティブ」状態で、セカンダリ サーバーが「セカンダリ同期」状態になっているときに、次の手順に従います。

ステップ 1 HA を削除します（CLI での HA の削除 （57 ページ）およびGUI での HA の削除 （56 ページ）を参照）。
ステップ 2 プライマリ サーバーとセカンダリ サーバーの両方が「HA 未設定」の状態になったら、HA を登録します。ハイ アベイラビリティのセットアップ （19 ページ） を参照してください

ハイ アベイラビリティの参照情報

以下の項に、HA に関する参照情報を記載します。

関連トピック

HA コンフィギュレーション モード リファレンス （52 ページ）
HA 状態リファレンス （52 ページ）
HA 状態遷移リファレンス （54 ページ）
ハイ アベイラビリティ CLI コマンド リファレンス （56 ページ）
HA 認証キーのリセット （56 ページ）
GUI での HA の削除 （56 ページ）
CLI での HA の削除 （57 ページ）
復元中の HA の削除 （57 ページ）
アップグレード中の HA の削除 （58 ページ）
HA エラー ロギングの使用 （59 ページ）
HA サーバーの IP アドレスまたはホスト名のリセット （59 ページ）

HA コンフィギュレーション モード リファレンス

次の表に、すべての可能な HA コンフィギュレーション モードを示します。

表 2: ハイ アベイラビリティ モード

モード	説明
HA 未設定（HA not configured）	HA は、この Prime Infrastructure サーバーに設定されていません。
HA 初期化中（HA initializing）	プライマリ サーバーとセカンダリ サーバー間の HA 登録プロセスが開始されました。
HA enabled	プライマリ サーバーとセカンダリ サーバー間で HA が有効になりました。
HA alone	プライマリ サーバーは単独で実行されています。HA は有効ですが、プライマリ サーバーがセカンダリ サーバーと同期していないか、セカンダリ サーバーがダウンしているか、またはセカンダリ サーバーに到達できません。

関連トピック

ハイ アベイラビリティの参照情報 （51 ページ）

HA 状態リファレンス

次の表に、ユーザーによる応答が必要ない状態も含め、すべての可能な HA 状態をリストします。

表 3: ハイ アベイラビリティ状態

状態	Server	説明
スタンドアロン（Stand Alone）	両方	HA は、この Prime Infrastructure サーバーに設定されていません。
プライマリ単独（Primary Alone）	プライマリ	プライマリ サーバーは、セカンダリ サーバーを失った後に再起動しました。Health Monitor のみがこの状態で稼働します。
HA 初期化中（HA Initializing）	両方	プライマリ サーバーとセカンダリ サーバー間の HA 登録プロセスが開始されました。
プライマリアクティブ（Primary Active）	プライマリ	プライマリ サーバーは現在アクティブであり、セカンダリ サーバーと同期中です。

状態	Server	説明
プライマリデータベースのコピー失敗（Primary Database Copy Failed）	プライマリ	再起動されるプライマリ サーバーは、自身が24時間以上ダウンしていたためにデータ ギャップが生じていないかを常に確認します。そして、このようなギャップを検出すると、自動的にアクティブなセカンダリ サーバーからのデータ コピーをトリガーします。まれに、このデータベースのコピーに失敗することがあります。そのような場合に、この遷移状態がプライマリ サーバーに設定されます。データベース コピーが正常に終了するまで、プライマリへのフェールバックの試行はすべてブロックされます。データベース コピーが正常に終了するとすぐに、プライマリ サーバーの状態が「プライマリ同期中（Primary Syncing）」に設定されます。
プライマリフェールオーバー（Primary Failover）	プライマリ	プライマリ サーバーで障害が検出されました。
プライマリフェールバック（Primary Failback）	プライマリ	ユーザーによってトリガーされたフェールバックが進行中です。
プライマリがセカンダリとの接続を喪失（Primary Lost Secondary）	プライマリ	プライマリ サーバーは、セカンダリ サーバーと通信できません。
プライマリがフェールバックの準備中（Primary Preparing for Failback）	プライマリ	セカンダリへのフェールオーバー後、プライマリ サーバーの起動時にこの状態が設定されます。この状態は、プライマリ サーバーがスタンバイ モード（セカンダリ サーバーがアクティブであるため）で起動し、フェールバックの準備ができていることを示します。プライマリ サーバーがフェールバックの準備ができると、その状態は「プライマリ同期中（Primary Syncing）」に設定されます。
プライマリ同期中（Primary Syncing）	プライマリ	プライマリ サーバーは、データベースおよびコンフィギュレーション ファイルを、アクティブなセカンダリ サーバーと同期しています。セカンダリ サーバーにフェールオーバーし、セカンダリ サーバーがアクティブ ロールを引き継いだ後、プライマリ プロセスが送り込まれてくるときに、プライマリ サーバーがこの状態に移行します。
プライマリの状態を確認不能（Primary Uncertain）	プライマリ	プライマリ サーバーのアプリケーション プロセスがデータベースに接続できません。
セカンダリ単独（Secondary Alone）	セカンダリ	プライマリ サーバーの再起動後、セカンダリ サーバーからプライマリ サーバーに接続できません。
セカンダリ同期中（Secondary Syncing）	セカンダリ	セカンダリ サーバーは、プライマリ サーバーとデータベースおよびコンフィギュレーション ファイルを同期しています。
セカンダリアクティブ（Secondary Active）	セカンダリ	プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが正常に完了しました。

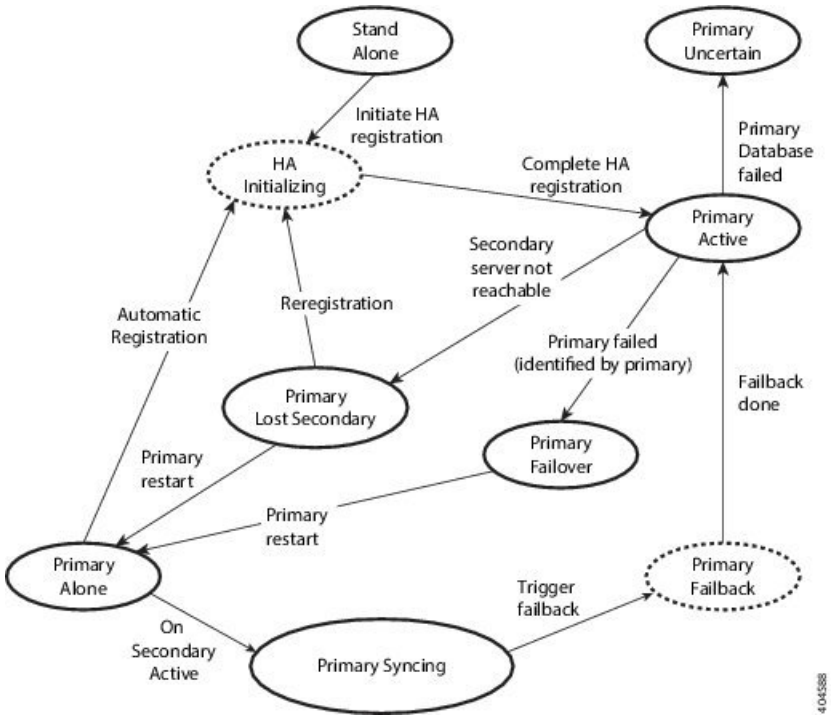
状態	Server	説明
セカンダリがプライマリとの接続を喪失（Secondary Lost Primary）	セカンダリ	セカンダリ サーバーがプライマリ サーバーに接続できません（この状態は、プライマリ サーバーで障害が発生した場合、またはネットワーク接続が失われた場合に発生します）。 この状態から自動フェールオーバーが行われる場合、セカンダリ サーバーは自動的に [Active] 状態に移ります。手動フェールオーバーの場合は、ユーザーがフェールオーバーをトリガーしてセカンダリ サーバーをアクティブにすることができます。
セカンダリフェールオーバー（Secondary Failover）	セカンダリ	フェールオーバーがトリガーされて進行中です。
セカンダリフェールバック（Secondary Failback）	セカンダリ	フェールバックがトリガーされて進行中です（データベースおよびファイル レプリケーションが進行中）。
セカンダリ ポスト フェールバック（Secondary Post Failback）	セカンダリ	この状態が発生するのは、フェールバックがトリガーされて、セカンダリ サーバーからプライマリ サーバーへのデータベースおよびコンフィギュレーション ファイルの複製が完了し、Health Monitor がセカンダリ サーバーの [Secondary Syncing] への状態遷移およびプライマリ サーバーの [Primary Active] への状態遷移を開始した場合です。この状態は、これらの状態変更および関連するプロセスの開始と停止が進行中であることを示します。
セカンダリの状態を確認不能（Secondary Uncertain）	セカンダリ	セカンダリ サーバーのアプリケーション プロセスが、セカンダリ サーバーのデータベースに接続できません。

関連トピック

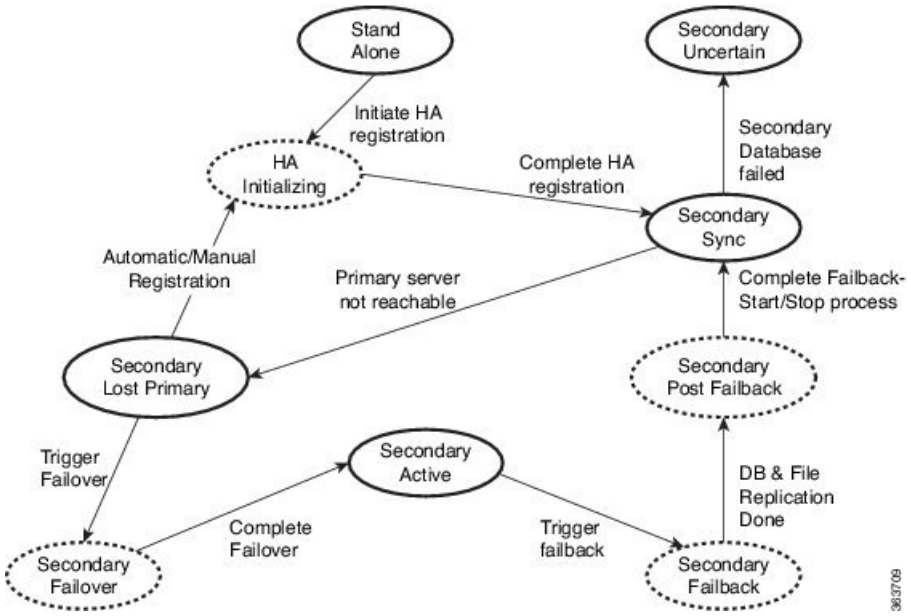
ハイ アベイラビリティの参照情報 （51 ページ）

HA 状態遷移リファレンス

次の図は、プライマリ サーバーのすべての可能な状態遷移を詳しく説明しています。



次の図は、セカンダリ サーバーのすべての可能な状態遷移を詳しく説明しています。



関連トピック

ハイ アベイラビリティの参照情報 （51 ページ）

ハイ アベイラビリティ CLI コマンド リファレンス

次の表に、HA 管理に使用できる CLI コマンドをリストします。これらのコマンドを実行するには、管理者としてプライマリ サーバーにログインします（「CLI から接続する方法」を参照）。

表 4: ハイ アベイラビリティ コマンド

コマンド	説明
ncs ha ?	ハイ アベイラビリティ CLI コマンドのヘルプを取得します。
ncs ha authkey authkey	ハイ アベイラビリティの認証キーを更新します。
ncs ha remove	ハイ アベイラビリティ構成を削除します。
ncs ha status	ハイ アベイラビリティの現在の状態を取得します。

関連トピック

ハイ アベイラビリティの参照情報 （51 ページ）

HA 認証キーのリセット

Prime Infrastructure 管理者は、**ncs ha authkey** コマンドを使用して HA 認証キーを変更できます。新しい認証キーがパスワード標準を満たすようにする必要があります。

ステップ 1 CLI を使用してプライマリ サーバーに接続します。「configure terminal」モードにしないでください。

ステップ 2 コマンドラインに次のように入力します。

admin# **ncs ha authkey** *MyNewAuthKey*

ここで、*MyNewAuthKey* は新しい認証キーです。詳細については、CLI から接続する方法を参照してください。

関連トピック

ハイ アベイラビリティをセットアップする前に （19 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

GUI での HA の削除

既存の HA 実装を削除するには、以下の手順で説明するように、GUI を使用するのが最も簡単な方法です。また、コマンド ラインから HA 設定を削除することもできます。

この方法を使用するには、プライマリ Prime Infrastructure サーバーの状態が「プライマリ アクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ

サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 管理者権限を持つユーザー ID を使用してプライマリ Prime Infrastructure サーバーにログインします。

ステップ 2 [管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]>[HA 設定（HA Configuration）] の順に選択します。

ステップ 3 [削除（Remove）] を選択します。HA 設定の削除には 3 ～ 4 分かかります。

削除が完了したら、ページに表示されている HA 設定モードが「HA 未設定（HA not Configured）」になっていることを確認します。

関連トピック

CLI での HA の削除 （57 ページ）
フェールバックのトリガー方法 （38 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

CLI での HA の削除

何らかの理由でプライマリ サーバー上の Prime Infrastructure GUI にアクセスできない場合、管理者は以下の手順に従い、コマンド ラインから HA 設定を削除することができます。

この方法を使用するには、プライマリ Prime Infrastructure サーバーの状態が「プライマリ アクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 CLI を使用してプライマリ サーバーに接続します。「configure terminal」モードにしないでください。

ステップ 2 コマンドラインに次のように入力します。

admin# **ncs ha remove**。詳細については、CLI から接続する方法を参照してください。

関連トピック

GUI での HA の削除 （56 ページ）
フェールバックのトリガー方法 （38 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

復元中の HA の削除

Prime Infrastructure は、ハイ アベイラビリティ関連の各種設定をバックアップしません。

HA を使用した Prime Infrastructure 実装を復元するには、必ず、バックアップしたデータをプライマリ サーバーのみに復元してください。復元されたプライマリ サーバーは、そのデータ

を自動的にセカンダリ サーバーに複製します。セカンダリ サーバーで復元操作を実行する必要はありません。これを実行しようとすると、エラー メッセージが生成されます。

HA を使用する Prime Infrastructure 実装を復元するには、次の手順に従います。

ステップ 1 GUI を使用して、プライマリ サーバーから HA 設定を削除します（「関連項目」の「GUI からの HA の削除」を参照）。

ステップ 2 必要に応じてプライマリ サーバーを復元します。

ステップ 3 復元が完了したら、HA 登録プロセスを再度実行します。

詳細については、データの復元およびCLI から接続する方法を参照してください。

関連トピック

GUI での HA の削除 （56 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

アップグレード中の HA の削除

HA を使用した Prime Infrastructure 実装をアップグレードするには、以下の手順に従います。

ステップ 1 GUI を使用して、プライマリ サーバーから HA 設定を削除します（「関連項目」の「GUI からの HA の削除」参照）。

ステップ 2 必要に応じてプライマリ サーバーをアップグレードします。

ステップ 3 現在のイメージを使用してセカンダリ サーバーを再インストールします。

セカンダリ サーバーを以前のバージョンやベータ版からアップグレードすることはできません。セカンダリ サーバーは常に新規インストールでなければなりません。

ステップ 4 アップグレードが完了したら、HA 登録プロセスを再度実行します。

（注） アップグレード後、ヘルス モニター ページに以下のヘルス モニター イベント メッセージが表示されます。

プライマリ認証キーが管理者によって変更されました（Primary Authentication Key was changed by Admin）

詳細については、CLI から接続する方法を参照してください。

関連トピック

GUI での HA の削除 （56 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

HA エラー ロギングの使用

ハイ アベイラビリティ機能に対するエラー ロギングは、ディスク スペースを節約し、最大限のパフォーマンスを達成するために、デフォルトで無効にされます。HAに問題がある場合は、まず、エラー ロギングを有効にして、記録されたログ ファイルを調べることから始めるのが最善です。

ステップ 1 問題のあるサーバーの Health Monitor ページを表示します。

ステップ 2 [ロギング（Logging）] 領域で、[メッセージ レベル（Message Level）] ドロップダウンから必要なエラー ロギング レベルを選択します。

ステップ 3 **[Save（保存）]** をクリックします。

ステップ 4 ログ ファイルをダウンロードする必要がある場合は、[Logs] 領域で、[Download] をクリックします。ダウンロードしたログ ファイルは、任意の ASCII テキスト エディタを使用して開くことができます。

関連トピック

ヘルス モニター Web ページへのアクセス （37 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

HA サーバーの IP アドレスまたはホスト名のリセット

プライマリまたはセカンダリ HA サーバーの IP アドレスまたはホスト名は、できるだけ変更しないようにしてください。IPアドレスまたはホスト名を変更しなければならない場合は、変更を行う前に、プライマリ サーバーから HA 設定を削除します。変更が終わったら、HA を再登録します。

関連トピック

GUI での HA の削除 （56 ページ）
プライマリ サーバーでの HA の登録方法 （22 ページ）
ハイ アベイラビリティの参照情報 （51 ページ）

任意の状態の TOFU エラーの解決

プライマリサーバーとセカンダリサーバーが通信する場合、次のTOFUエラーが発生する可能性があります。

続行する前に、次のエラーを修正する必要があります。「この接続には、ゼロトラスト（*TOFU*）ベースの証明書が設定されています。リモートホストの現在の証明書は、以前に使用されていたものとは異なります。（*A Trust-on-first-use (TOFU) based Certificate is configured for this connection. The current certificate on the remote host is different than what was used earlier.*」

この問題を修正するには、次の手順を実行する必要があります。

- プライマリサーバーとセカンダリサーバーの両方で NCS CLI コマンドを使用して既存の証明書をクリアします。

```
ncs certvalidation tofu-certs deletecert host <server-hostname>
```

MSE ハイ アベイラビリティの設定

Cisco Mobility Services Engine（MSE）は、複数のモビリティ アプリケーションをホストするプラットフォームです。MSE ハイ アベイラビリティ（HA）設定の下では、アクティブな MSE は MSE の別の非アクティブ インスタンスによりバックアップされます。アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （60 ページ）
MSE ハイ アベイラビリティのセットアップ：ワークフロー （63 ページ）

MSE ハイ アベイラビリティ アーキテクチャの概要

MSE ハイ アベイラビリティ システムの主要なコンポーネントは、ヘルス モニターです。ヘルス モニターは、各 MSE での HA セットアップの設定、管理、モニターを行います。プライマリ MSE とセカンダリ MSE の間でハートビートが維持されます。ヘルス モニターは、データベースのセットアップ、ファイルのレプリケーション、アプリケーションのモニタリングを行います。プライマリ MSE で障害が発生し、セカンダリ MSE に切り替わると、プライマリ MSE の仮想アドレスがセカンダリ MSE に透過的に切り替わります。次の点に注意してください。

- アクティブな各プライマリ MSE は別の非アクティブ インスタンスによりバックアップされます。セカンダリ MSE の目的は、プライマリ MSE のアベイラビリティと状態をモニターすることです。セカンダリ MSE は、フェールオーバー手順の開始後にアクティブになります。
- 1 つのセカンダリ MSE で 1 つのプライマリ MSE をサポートできます。

[Services] タブの [MSE]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context-Aware Notifications]、および [Mobile Concierge] ページは、リリース 7.3 の仮想ドメインのみで使用できます。

以下の関連項目は、MSE ハイ アベイラビリティ アーキテクチャに関する追加の詳細情報を提供します。

関連トピック

MSE ハイ アベイラビリティのペアリング マトリックス （61 ページ）
MSE ハイ アベイラビリティのガイドラインと制約事項 （61 ページ）
MSE ハイ アベイラビリティのフェールオーバー シナリオ （62 ページ）
MSE ハイ アベイラビリティのフェールバック シナリオ （62 ページ）
MSE ハイ アベイラビリティのライセンス要件 （63 ページ）
MSE ハイ アベイラビリティの設定 （60 ページ）

MSE ハイ アベイラビリティのペアリング マトリックス

次の表は、ハイ アベイラビリティ構成においてペアリング可能な MSE サーバーのタイプを一覧表示しています。

表 *5 : MSE* ハイ アベイラビリティ サーバーのペアリング マトリックス

プライマリ サーバー タイプ	セカンダリ サーバー タイプ				
3355	VA-2	VA-3	VA-4	VA-5	
3355	あり	なし	なし	なし	なし
VA-2	なし	あり	あり	あり	あり
VA-3	なし	なし	あり	あり	あり
VA-4	なし	なし	なし	あり	あり
VA-5	なし	なし	なし	なし	あり

関連トピック

リモート モデルの使用 （14 ページ）
MSE ハイ アベイラビリティのガイドラインと制約事項 （61 ページ）

MSE ハイ アベイラビリティのガイドラインと制約事項

MSE ハイ アベイラビリティを実装し、これを Prime Infrastructure から管理する予定の管理者は、以下のガイドラインと制限事項に従う必要があります。

- ヘルス モニター IP と仮想 IP の両方に Prime Infrastructure からアクセスできるようにする必要があります。
- ヘルス モニター IP と仮想 IP は常に異なる IP でなければなりません。ヘルス モニターと仮想インターフェイスは、同じネットワーク インターフェイス上にあっても別のインターフェイス上にあってもかまいません。
- 手動フェールオーバーと自動フェールオーバーのいずれかを使用できます。フェールオーバーは、一時的なものであると見なす必要があります。故障した MSE をできるだけ早く復旧して、フェールバックを再開する必要があります。故障した MSE の復旧に時間がかかるほど、ハイ アベイラビリティのサポートなしで単一 MSE を稼働する時間が長くなります。
- 手動フェールバックと自動フェールバックのいずれかを使用できます。
- プライマリ MSE とセカンダリ MSE は、同じソフトウェア バージョンを実行する必要があります。

- WAN 上のハイ アベイラビリティはサポートされません。
- LAN 上のハイ アベイラビリティは、プライマリ MSE とセカンダリ MSE の両方が同じサブネット内にある場合に限りサポートされます。
- プライマリとセカンダリのMSEが通信するポートを開ける（ネットワーク ファイアウォール、アプリケーション ファイアウェイ、ゲートウェイなどでブロックしない）必要があります。次の入力/出力ポートを開く必要があります：80、443、8080、8081、22、8001、1521、1411、1522、1523、1524、1525、9006、15080、61617、59000、12091、1621、1622、1623、1624、1625、8083、8084、8402。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （60 ページ）
MSE ハイ アベイラビリティのペアリング マトリックス （61 ページ）
MSE ハイ アベイラビリティのフェールオーバー シナリオ （62 ページ）

MSE ハイ アベイラビリティのフェールオーバー シナリオ

プライマリ MSE で障害が検出されると、次のイベントが発生します。

- セカンダリ MSEのヘルス モニターにより、プライマリ MSEが機能していないこと（ハードウェア障害、ネットワーク障害など）が確認されます。
- 自動フェールオーバーが有効化されている場合、即座にセカンダリ MSE が起動します。
- 手動フェールオーバーが有効化されている場合は、フェールオーバーを手動で開始するかどうかを確認する電子メールが管理者に送信されます。この電子メールは、MSE アラーム用に電子メールが設定されている場合のみ送信されます。
- フェールオーバー動作の結果はヘルス モニター UI でイベントとして示され、クリティカル アラームが Prime Infrastructure に送信されます。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （60 ページ）
MSE ハイ アベイラビリティのガイドラインと制約事項 （61 ページ）
MSE ハイ アベイラビリティのフェールバック シナリオ （62 ページ）

MSE ハイ アベイラビリティのフェールバック シナリオ

セカンダリ MSE がすでにプライマリ MSE のフェールオーバー状態である場合、プライマリ MSE が通常の状態に戻ると、フェールバックを呼び出すことができます。

フェールバックが発生するのは、セカンダリ MSE がプライマリ インスタンスに対して次のいずれかの状態である場合だけです。

- セカンダリ MSE が実際にプライマリ MSE をフェールオーバーしている。
- 手動フェールオーバーが設定されているが、管理者が呼び出さなかった。
- プライマリ MSE で障害が発生したが、エラーが発生したため、セカンダリ MSE が引き継ぐことができない。
- フェールバックは、障害が発生したプライマリ MSE を管理者が起動する場合にだけ行われます。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （60 ページ）
MSE ハイ アベイラビリティのフェールオーバー シナリオ （62 ページ）
MSE ハイ アベイラビリティのライセンス要件 （63 ページ）

MSE ハイ アベイラビリティのライセンス要件

ハイ アベイラビリティでは、プライマリおよびセカンダリ仮想アプライアンスでアクティベーション ライセンスが必要です。他のサービスのライセンスはセカンダリ MSE に必要ありません。プライマリ MSE のみで必要です。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （60 ページ）
MSE ハイ アベイラビリティのフェールバック シナリオ （62 ページ）

MSE ハイ アベイラビリティのセットアップ：ワークフロー

MSE ソフトウェアのインストール中（または MSE セットアップ スクリプトの使用中）に、所定の重要な要素を設定します。Prime Infrastructure UI からプライマリ MSE とセカンダリ MSE を組み合わせます。

デフォルトでは、すべての MSE がプライマリとして設定されます。ハイ アベイラビリティ サポートを使用しない場合、および以前のリリースからのアップグレードを実行している場合は、引き続きその MSE の IP アドレスを使用してください。ハイ アベイラビリティをセットアップするには、ヘルス モニターの IP アドレスを設定する必要があります。したがって、ヘルス モニターが仮想 IP アドレスになります。

MSE ハイ アベイラビリティの設定は、次の手順で構成されています。

1. ハイ アベイラビリティ用の MSE の準備
2. プライマリ MSE の設定
3. セカンダリ MSE の設定

プライマリ MSE サーバーの交換が必要な場合には、MSE ハイ アベイラビリティの再設定が必要になることもあります。

詳細については、下記の該当する関連項目を参照してください。

関連トピック

ハイ アベイラビリティ用の MSE の準備 （64 ページ）
プライマリ MSE での MSE ハイ アベイラビリティの設定 （64 ページ）
セカンダリ MSE での MSE ハイ アベイラビリティの設定 （72 ページ）
プライマリ MSE の交換 （78 ページ）
MSE ハイ アベイラビリティの設定

ハイ アベイラビリティ用の MSE の準備

プライマリおよびセカンダリ MSE をハイ アベイラビリティ用に準備するには、次の手順に従ってください。

ステップ 1 プライマリ MSE とセカンダリ MSE の間のネットワーク接続が機能しており、すべての必要なポートが開いていることを確認します。

ステップ 2 正しいバージョンの MSE をプライマリ MSE 上にインストールします。

ステップ 3 同じバージョンの MSE がセカンダリ MSE にインストールされていることを確認します。

関連トピック

プライマリ MSE の交換 （78 ページ）
MSE ハイ アベイラビリティの設定 （60 ページ）

プライマリ MSE での MSE ハイ アベイラビリティの設定

プライマリ MSE をハイ アベイラビリティ用に設定するには、次の手順に従ってください。

ステップ 1 プライマリ MSE で次のコマンドを入力します。

/opt/mse/setup/setup.sh

セットアップ スクリプトにより、次のような入力要求が表示されます。用意された選択肢を使って太字で回答できます（このステップおよび次のステップが対象）。

```
------------------------------------------------------------
Welcome to the Cisco Mobility Services Engine Appliance Setup.
You may exit the setup at any time by typing <Ctrl+c>.
------------------------------------------------------------
Would you like to configure MSE using:
1. Menu mode
2. Wizard mode
Choose 1 or 2: 1
------------------------------------------------
Mobility Services Engine Setup
Please select a configuration option below and enter the requested information. You may exit setup at any time by typing <Ctrl +C>.
You will be prompted to choose whether you wish to configure a parameter, skip it, or reset it to its initial default value. Skipping a parameter will leave it unchanged from its current value.
Please note that the following parameters are mandatory and must be configured at lease once.
-> Hostname
```

-> Network interface eth0

-> Timezone settings

-> Root password

-> NTP settings

-> Prime Infrastructure password

You must select option 24 to verify and apply any changes made during this session.

PRESS <ENTER> TO CONTINUE:

Configure MSE:

1) Hostname * 13) Remote syslog settings

2) Network interface eth0 settings* 14) Host access control settings

3) Timezone settings* 15) Audit Rules

4) Root password * 16) Login banner

5) NTP settings * 17) System console restrictions

6) Prime Infrastructure password * 18) SSH root access

7) Display current configuration 19) Single user password check

8) Domain 20) Login and password settings

9) High availability role 21) GRUB password

10) Network interface eth1 settings 22) Root access control

11) DNS settings 23) Auto start MSE on system boot up

12) Future restart time 24) ## Verify and apply changes ##

Please enter your choice [1 - 24]:

ステップ 2 プライマリ MSE のホスト名を設定します。

Please enter your choice [1 - 24]: **1**

Current Hostname=[mse]

Configure Hostname? (Y)es/(S)kip/(U)se default [Skip]: **y**

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Enter a Host name [mse]:**mse1**

ステップ 3 プライマリ MSE のドメインを設定します。

Please enter your choice [1-24]: **8**

Current domain=[ ]

Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: **S**

ステップ 4 プライマリ MSE ネットワーク インターフェイス eth0 を設定します。

Please enter your choice [1 - 24]: **2**

Current eth0 interface IP address=[10.0.0.1]

Current eth0 interface netmask=[255.0.0.0]

Current IPv4 gateway address=[172.20.104.123]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: **y**

Enter an IP address for first Ethernet interface of this machine.

Enter eth0 IP address [10.0.0.2]:

Enter the network mask for IP address 172.21.105.126

Enter network mask [255.255.255.224]:

Enter the default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface.

Enter default gateway address [172.20.104.123]:

ステップ 5 プライマリ MSE のルート パスワードを設定します。

Please enter your choice [1 - 24]: **4**

Root password has not been configured

Configure root password? (Y)es/(S)kip/(U)se default [Skip]: **y**

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use an 8 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

Enter new password: **password**

ステップ 6 プライマリ MSE のハイ アベイラビリティ ロールを設定します。

Current role=[Primary]

Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: **y**

High availability role for this MSE (Primary/Secondary)

Select role [1 for Primary, 2 for Secondary] [1]: 1

Health monitor interface holds physical IP address of this MSE server.

This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves

Select Health Monitor Interface [eth0/eth1] [eth0]: eth0

Direct connect configuration facilitates use of a direct cable connection between the primary and secondary MSE servers.

This can help reduce latencies in heartbeat response times, data replication and failure detection times.

Please choose a network interface that you wish to use for direct connect. You should appropriately configure the respective interfaces.

"none" implies you do not wish to use direct connect configuration.

Select direct connect interface [eth0/eth1/none] [none]:

Enter a Virtual IP address for the Primary MSE server

Enter Virtual IP address [1.1.1.1]: **10.10.10.11**

Enter network mask for IP address 10.10.10.1

Enter network mask [1.1.1.1]: **255.255.255.0**

Select to start the server in recovery mode.

You should choose yes only if this primary MSE was paired earlier and you have now lost the configuration from this box.

And, now you want to restore the configuration from Secondary via Cisco Prime Infrastructure

Do you wish to start this MSE in HA receovery mode?: (yes/no} [no]:no

Current IP address = [1.1.1.10]

Current eth0 netmask=[255.255.255.0]

Current gateway address=[1.1.1.1]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

Enter an IP address for first Ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: **10.10.10.12**

Enter the network mask for IP address 10.10.10.12

Enter network mask [255.255.255.0]: **255.255.255.0**

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface. Enter default gateway address [1.1.1.1]:**10.10.10.1**

The second Ethernet interface is currently disabled for this machine.

Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S

ステップ 7 プライマリ MSE のタイムゾーンを設定します。

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly. Please select a continent or ocean.

1) Africa

2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) UTC - I want to use Coordinated Universal Time.
#? 2
Please select a country.
1) Anguilla 27) Honduras
2) Antigua & Barbuda
5) Bahamas 31) Montserrat
6) Barbados 32) Netherlands Antilles
7) Belize 33) Nicaragua
8) Bolivia 34) Panama
9) Brazil 35) Paraguay
10) Canada 36) Peru
11) Cayman Islands 37) Puerto Rico
12) Chile 38) St Barthelemy
13) Colombia 39) St Kitts & Nevis
14) Costa Rica 40) St Lucia
41) St Martin（フランス語）
16) Dominica 42) St Pierre & Miquelon
17) Dominican Republic 43) St Vincent
18) Ecuador 44) Suriname
19) El Salvador 45) Trinidad & Tobago
20) French Guiana 46) Turks & Caicos Is
21) Greenland 47) United States
22) Grenada 48) Uruguay
23) Guadeloupe 49) Venezuela
24) Guatemala 50) Virgin Islands (UK)

25) Guyana 51) Virgin Islands (US)

26) Haiti

#? 47

Please select one of the following time zone regions.

1) Eastern Time

2) Eastern Time - Michigan - most locations

3) Eastern Time - Kentucky - Louisville area

4) Eastern Time - Kentucky - Wayne County

5) Eastern Time - Indiana - most locations

6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties

7) Eastern Time - Indiana - Pulaski County

8) Eastern Time - Indiana - Crawford County

9) Eastern Time - Indiana - Pike County

10) Eastern Time - Indiana - Switzerland County

12) Central Time - Indiana - Perry County

13) Central Time - Indiana - Starke County

14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties

15) Central Time - North Dakota - Oliver County

16) Central Time - North Dakota - Morton County (except Mandan area)

18) Mountain Time - south Idaho & east Oregon

20) Mountain Standard Time - Arizona

21) Pacific Time

22) Alaska Time

23) Alaska Time - Alaska panhandle

24) Alaska Time - Alaska panhandle neck

25) Alaska Time - west Alaska

26) Aleutian Islands

27) Hawaii

#? 21

The following information has been given:

United States

Pacific Time

Therefore TZ='America/Los_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2020. Universal Time is now: Mon Apr 7 01:45:27 UTC 2020. Is the above information OK?

1) Yes

2) No

#? 1

ステップ 8 プライマリ MSE の DNS を設定します。

Please enter your choice [1 - 24]: 11

Domain Name Service (DNS) Setup

Enable DNS (yes/no) [no]: y

Default DNS server 1=[8.8.8.8]

Enter primary DNS server IP address:

DNS server address must be in the form #.#.#.#, where # is 0 to 255 or hexadecimal :

separated v6 address

Enter primary DNS server IP address [8.8.8.8]:

Enter backup DNS server IP address (or none) [none]:

ステップ 9 プライマリ MSE の NTP を設定します。

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the

Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :

separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

ステップ 10 Prime Infrastructure パスワードを設定します。

Please enter your choice [1 - 24]: 6

Cisco Prime Infrastructure communication password has not been configured. Configure Prime Infrastructure password? (Y)es/(S)kip/(U)se default [Yes]:

Enter a password for the admin user.

The admin user is used by the Prime Infrastructure and other northbound systems to authenticate their SOAP/XML session with the server. Once this password is updated, it must correspondingly be updated on the NCS page for MSE General Parameters so that the Prime Infrastructure can communicate with the MSE.

ステップ 11 変更を確認して適用します。

Please enter your choice: 24

Please verify the following setup information.

----------BEGIN---------- Hostname=mse1

Role= 1, Health Monitor Intercace=eth0, Direct connect interface=none

Virtual IP Address=10.10.10.11, Virtual IP Netmask=255.255.255.0

Eth0 IP address=10.10.10.12, Eth0 network mask=255.0.0.0

Default Gateway=10.10.10.1

Time zone=America/Los_Angeles

Enable DNS=yes, DNS servers=8.8.8.8

Enable NTP=yes, NTP servers=time.nist.gov

Time zone=America/Los_Angeles

Root password is changed.

Cisco Prime Infrastructure password is changed.

----------END----------

You may enter "yes" to proceed with configuration, "no" to make

more changes.

Configuration Changed

Is the above information correct (yes or no): yes

Checking mandatory configuration information...

Root password: Not configured

WARNING

The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes

Setup will now attempt to apply the configuration. Restarting network services with new settings. Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

ステップ 12 システムを再起動します。

[root@mse1]# reboot Stopping MSE Platform

Flushing firewall rules: [OK]

Setting chains to policy ACCEPT: nat filter [OK] Unloading iptables modules: [ok]

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

ステップ 13 MSE サービスを開始します。

[root@mse1]# /etc/init.d/msed start

Starting MSE Platform.

Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting to check the status. Health Monitor successfully started

Starting Admin process... Started Admin process. Starting database .....

Database started successfully. STarting framework and services..... Framework and services successfully started

ステップ 14 すべてのサービスが開始された後、次のコマンドを入力して、MSE サービスが正常に動作していることを確認します。

[root@mse1]# getserverinfo

関連トピック

ハイ アベイラビリティ用の MSE の準備 （64 ページ）
セカンダリ MSE での MSE ハイ アベイラビリティの設定 （72 ページ）
MSE ハイ アベイラビリティの設定 （60 ページ）

セカンダリ MSE での MSE ハイ アベイラビリティの設定

セカンダリ MSE をハイ アベイラビリティ用に準備するには、次の手順に従ってください。

ステップ 1 目的のセカンダリ MSE で次のコマンドを入力します。

/opt/mse/setup/setup.sh

セットアップ スクリプトにより、プライマリ MSE の場合と同じ入力要求が表示されます。

ステップ 2 セカンダリ MSE のホスト名を設定します。

Please enter your choice [1 - 24]: **1**

Current hostanme=[mse1]

Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: yes

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Enter a hostname [mse]: **mse2**

ステップ 3 セカンダリ MSE のドメインを設定します。

Please enter your choice [1-24]: 8

Current domain=[ ]

Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: S

ステップ 4 セカンダリ MSE のハイ アベイラビリティ ロールを設定します。

Current role=[Primary]

Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: High availability role for this MSE (Primary/Secondary)

Select role [1 for Primary, 2 for Secondary] [1]: 2

Health monitor interface holds physical IP address of this MSE server.

This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves

Select Health Monitor Interface [eth0/eth1] [eth0]: eth0

Direct connect configuration facilitates use of a direct cable connection between the primary and secondary MSE servers.This can help reduce latencies in heartbeat response times, data replication and failure detection times.Please choose a network interface that you wish to use for direct connect. You should appropriately configure the respective interfaces.

"none" implies you do not wish to use direct connect configuration.

Select direct connect interface [eth0/eth1/none] [none]:

Current IP address=[1.1.1.10]

Current eth0 netmask=[255.255.255.0] Current gateway address=[1.1.1.1]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:

Enter an IP address for first Ethernet interface of this machine. Enter eth0 IP address [1.1.1.10]: 10.10.10.13

Enter the network mask for IP address 10.10.10.13

Enter network mask [255.255.255.0]:

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface. Enter default gateway address [1.1.1.1]:10.10.10.1

The second Ethernet interface is currently disabled for this machine. Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S

ステップ 5 セカンダリ MSE のタイムゾーンを設定します。

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly. Please select a continent or ocean.

1) Africa

2) Americas

3) Antarctica

4) Arctic Ocean

5) Asia

6) Atlantic Ocean

7) Australia

8) Europe

9) Indian Ocean

10) Pacific Ocean

11) UTC - I want to use Coordinated Universal Time.

#? 2

Please select a country.

1) Anguilla 27) Honduras

2) Antigua & Barbuda

5) Bahamas 31) Montserrat

6) Barbados 32) Netherlands Antilles

7) Belize 33) Nicaragua

8) Bolivia 34) Panama

9) Brazil 35) Paraguay

10) Canada 36) Peru

11) Cayman Islands 37) Puerto Rico

12) Chile 38) St Barthelemy

13) Colombia 39) St Kitts & Nevis

14) Costa Rica 40) St Lucia

41) St Martin（フランス語）

16) Dominica 42) St Pierre & Miquelon

17) Dominican Republic 43) St Vincent

18) Ecuador 44) Suriname

19) El Salvador 45) Trinidad & Tobago

20) French Guiana 46) Turks & Caicos Is

21) Greenland 47) United States

22) Grenada 48) Uruguay

23) Guadeloupe 49) Venezuela

24) Guatemala 50) Virgin Islands (UK)

25) Guyana 51) Virgin Islands (US)

26) Haiti

#? 47

Please select one of the following time zone regions.

1) Eastern Time

2) Eastern Time - Michigan - most locations

3) Eastern Time - Kentucky - Louisville area

4) Eastern Time - Kentucky - Wayne County

5) Eastern Time - Indiana - most locations

6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties

7) Eastern Time - Indiana - Pulaski County

8) Eastern Time - Indiana - Crawford County

9) Eastern Time - Indiana - Pike County

10) Eastern Time - Indiana - Switzerland County

11) Central Time

12) Central Time - Indiana - Perry County

13) Central Time - Indiana - Starke County

14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties

15) Central Time - North Dakota - Oliver County

16) Central Time - North Dakota - Morton County (except Mandan area)

17) Mountain Time

18) Mountain Time - south Idaho & east Oregon

19) Mountain Time - Navajo

20) Mountain Standard Time - Arizona

21) Pacific Time

22) Alaska Time

23) Alaska Time - Alaska panhandle

24) Alaska Time - Alaska panhandle neck

25) Alaska Time - west Alaska

26) Aleutian Islands

27) Hawaii

#? 21

The following information has been given: United States

Pacific Time

Therefore TZ='America/Los_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2014. Universal Time is now: Mon Apr 7 01:45:27 UTC 2014. Is the above information OK?

1) Yes

2) No

#? 1

ステップ 6 セカンダリ MSE の NTP を設定します。

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :

separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

ステップ 7 変更を確認して適用します。

Please enter your choice: 24

Please verify the following setup information.

----------BEGIN---------- Hostname=mse2

Role= 2, Health Monitor Intercace=eth0, Direct connect interface=none

Eth0 IP address=10.10.10.13, Eth0 network mask=255.255.255.0

Default Gateway=10.10.10.1

Time zone=America/Los_Angeles

Enable NTP=yes, NTP servers=time.nist.gov

Time zone=America/Los_Angeles

----------END----------

You may enter "yes" to proceed with configuration, "no" to make more changes.

Configuration Changed

Is the above information correct (yes or no): yes

Checking mandatory configuration information...

Root password: Not configured

WARNING

The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes

Setup will now attempt to apply the configuration.

Restarting network services with new settings. Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

ステップ 8 システムを再起動します。

[root@mse2 installers]# reboot

Stopping MSE Platform

Flushing firewall rules: [OK]

Setting chains to policy ACCEPT: nat filter [OK] Unloading iptables modules: [ok]

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

ステップ 9 MSE サービスを開始します。

[root@mse2]# /etc/init.d/msed start

Starting MSE Platform.

Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting to check the status. Health Monitor successfully started

Starting Admin process... Started Admin process. Starting database .....

Database started successfully. STarting framework and services..... Framework and services successfully started

関連トピック

ハイ アベイラビリティ用の MSE の準備 （64 ページ）
プライマリ MSE での MSE ハイ アベイラビリティの設定 （64 ページ）
MSE ハイ アベイラビリティの設定 （60 ページ）

プライマリ MSE の交換

何らかの理由でプライマリ MSE を交換する必要がある場合、以下の手順に従うことにより、現在のペアリング情報を新しく設定したプライマリ MSE にリカバリできます。

ステップ 1 セットアップ スクリプトを使用して、MSE をプライマリとして設定します。

ステップ 2 Prime Infrastructure を使用して、プライマリ MSE とセカンダリ MSE の間のペアリングをセットアップします。

ステップ 3 プライマリ MSE からセカンダリ MSE へのフェールオーバーを開始します。

ステップ 4 セットアップスクリプトを使用して、交換用MSEをプライマリとして設定します。新しいプライマリ MSE は、セカンダリ MSE とソフトウェアのバージョンが同じであり、古いプライマリ MSE と設定が同じであることが必要です。

ステップ 5 リカバリ モードを選択し、指示に従います。

ステップ 6 Prime Infrastructure を使用して、新しいプライマリ MSE へのフェールバックを開始します。

この新しいプライマリ MSEには新しいライセンスが必要です。最初のライセンスは新しいプライマリ MSE の UDI に一致しないため機能しません。

関連トピック

プライマリ MSE での MSE ハイ アベイラビリティの設定 （64 ページ）
MSE ハイ アベイラビリティの設定 （60 ページ）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。